WILLKIE FARR & GALLAGHER LLP
BENEDICT HUR (SBN 224018)
bhur@willkie.com
SIMONA AGNOLUCCI (SBN 246943)
sagnolucci@willkie.com
EDUARDO SANTACANA (SBN 281668)
esantacana@willkie.com
JOSHUA D. ANDERSON (SBN 312836)
jdanderson@willkie.com
DAVID D. DOAK (SBN 301319)
ddoak@willkie.com
TIFFANY LIN (SBN 321472)
tlin@willkie.com
HARRIS MATEEN (SBN 335593)
hmateen@willkie.com
NAIARA TOKER (SBN 346145)
ntoker@willkie.com
333 Bush Street, 34th Floor
San Francisco, California 94104
Telephone: (415) 858-7400

Attorneys for Defendant
GOOGLE LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE I, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-02431-VC
(Consol. w/ 3:32-cv-02343-VC)

DEFENDANT GOOGLE LLC'S STATEMENT OF RECENT DECISION

Judge: Hon. Vince Chhabria

First Am. Complaint Filed: November 16, 2023

DEFENDANT GOOGLE LLC'S STATEMENT OF RECENT DECISION

Pursuant to Civil Local Rule 7-3(d)(2), Defendant Google LLC respectfully submits for the Court's consideration the recent Order on Motion to Dismiss in *John Doe, et al., v Kaiser Foundation Health Plan, Inc., et al.*, No. 23-cv-02865-EMC (N.D. Cal. April 11, 2024), a true and correct copy of which is attached hereto as **Exhibit A**. The decision is relevant to Plaintiffs' claims for violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510*, et seq*., violation of the California Invasion of Privacy Act, Cal. Penal Code. § 630, *et seq*., invasion of privacy, Cal. Const. art. I, § 1, intrusion upon seclusion, breach of express contract, and breach of implied contract, which Google has moved to dismiss.

Dated: April 18, 2024

WILLKIE FARR & GALLAGHER LLP

By: */s/ Eduardo Santacana*
Benedict Hur
Simona Agnolucci
Eduardo Santacana
Joshua Anderson
David Doak
Tiffany Lin
Harris Mateen
Naiara Toker

Attorneys for Defendant
GOOGLE LLC

EXHIBIT A

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DOE, et al.,

Plaintiffs,

v.

KAISER FOUNDATION HEALTH PLAN, INC., et al.,

Defendants.

Case No. 23-cv-02865-EMC

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS

Docket No. 88

Plaintiffs are seven individuals who are proceeding anonymously: John Doe, John Doe II, Jane Doe, and Jane Does II-V.[1] They have filed suit on their own behalf and on the behalf of others similarly situated against three Kaiser entities: Kaiser Foundation Health Plan., Inc. ("KFHP"); Kaiser Foundation Hospitals ("Hospitals"); and The Permanente Medical Group ("TPMG"). Collectively, the Kaiser entities shall be referred to as "Kaiser." According to Plaintiffs, Kaiser installed code from third parties on its website and two mobile applications (*i.e.*, the Kaiser Permanente App and the Kaiser Permanente Washington App); that code allows the third parties "to intercept the content of [a Kaiser plan member's] patient status, identifying information, medical topics researched, choices made, information shared and communications with their medical providers, including personally identifiable medical information and other

[1] Specifically, Plaintiffs are: (1) John Doe, a citizen and resident of California, *see* FAC ¶ 13; (2) John Doe II, a citizen and resident of Georgia, *see* FAC ¶ 17; (3) Jane Doe, a citizen and resident of Washington, *see* FAC ¶ 21; (4) Jane Doe II, a citizen and resident of Washington, D.C., *see* FAC ¶ 25; (5) Jane Doe III, a citizen and resident of Maryland, *see* FAC ¶ 29; (6) Jane Doe IV, a citizen and resident of Virginia, *see* FAC ¶ 33; and (7) Jane Doe V, a citizen and resident of Oregon. *See* FAC ¶ 37.

confidential information and communications, when that information is in transit" (*i.e.*, between the Kaiser plan member and Kaiser). FAC ¶ 4. The third parties whose code is allegedly on the Kaiser website and mobile applications are: Quantum Metric, Twitter, Adobe, Bing, Google, and Dynatrace.[2]

Now pending before the Court is Kaiser's motion to dismiss. Kaiser has challenged each of the twenty-one claims asserted in the operative first amended complaint ("FAC"). All of the claims are class claims. In some instances, Plaintiffs have asserted claims on behalf of a multistate class (*i.e.*, a class consisting of people who live in the states where Kaiser operates, also referred to as the Kaiser Operating States Class). In other instances, Plaintiffs have asserted claims on behalf of a single state subclass. Plaintiffs have asserted a number of different claims. A few are based on the common law – *e.g.*, intrusion upon seclusion, breach of contract (express and implied), and negligence. Most are based on a statute. The statutes include wiretapping statutes, computer crime statutes, consumer protection statutes, and statutes similar to the federal Health Insurance Portability and Accountability Act ("HIPAA").

Having considered the parties' briefs as well as the oral argument of counsel, the Court hereby **GRANTS** in part and **DENIES** in part Kaiser's motion to dismiss.

I. FACTUAL & PROCEDURAL BACKGROUND

In the FAC, Plaintiffs allege as follows. KFHP, Hospitals, and TPMG operate under the trade name Kaiser Permanente. KFHP offers health care plans, with hospital care and physician care provided through hospitals and physician practices operated by Hospitals and TPMG. Altogether, Kaiser operates in nine jurisdictions: California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, Washington, and Washington, D.C. (referred to collectively as the "Kaiser Operating States"). *See* FAC ¶¶ 41-46. Plaintiffs and the members of the classes they seek to represent are members of Kaiser health plans in the various jurisdictions. *See* FAC ¶ 51.

Kaiser operates a website and two mobile applications. Through the website, Kaiser plan members "can perform various tasks that traditionally were only available by physically visiting

[2] Dynatrace seems to be implicated with respect to the Kaiser Permanente Washington App only. *See* FAC at 2 n.4; Malaga Decl. ¶ 5.

their health care providers' offices or speaking directly to their health care providers, such as scheduling appointments; checking medical results; reviewing medical histories; researching doctors, locations, and medical services; communicating with providers and paying medical bills." FAC ¶ 52. Members can do certain tasks, such as researching health conditions and finding doctors, without logging into a patient portal. *See* FAC ¶ 53. For other tasks, such as accessing medical information, scheduling appointments, and communicating with providers, members must log into the patient portal. *See* FAC ¶ 57. By signing into the patient portal, a Kaiser plan member agrees to the website and mobile application Terms and Conditions ("TAC") and related Privacy Statement. *See* FAC ¶ 64; *see also* FAC, Exs. 1-2 (TAC and Privacy Statement).

Similar to above, Kaiser plan members can also use mobile applications "to communicate with their doctor's office, schedule appointments, review information about past appointments, fill or refill prescriptions, view their medical history (including allergies, immunizations, ongoing health conditions, and lab test results), choose a doctor, and receive personalized reminders and health information." FAC ¶ 62.

Through the TAC and Privacy Statement, Kaiser expressly and impliedly promises Kaiser plan members that "it will maintain the privacy and confidentiality of the information shared, and the communications engaged in, on the Site, Portal, and mobile applications." FAC ¶ 73. But despite these promises, Kaiser intentionally

> installed code from multiple third parties throughout the Kaiser Permanente website and mobile applications that allows third party companies such as Quantum Metric, Twitter, Adobe, Bing, and Google [as well as Dynatrace] (collectively, "Third Party Wiretappers") to intercept the content of Plaintiffs and Class Members' patient status, identifying information, medical topics researched, choices made, information shared and communications with their medical providers, including personally identifiable medical information and other confidential information and communications, when that information is in transit [*i.e.*, between the member and Kaiser].

FAC ¶ 4.

Based on the allegations in the FAC, it appears that Kaiser installed the code from third parties so that Kaiser could use the information collected by the third parties for its own benefit. *See, e.g.*, FAC ¶ 108 (alleging that Adobe's "Experience Cloud . . . allow[s] businesses to

personalize and improve their marketing on websites, apps, and social media pages by collecting and analyzing information about website visitors"); FAC ¶ 142 (alleging that Twitter partners with companies such as Kaiser so that the partner "can use [Twitter's] analytic tools for marketing").

However, it also appears that third parties used the information collected for their own benefit and not just Kaiser's. *See, e.g.*, FAC ¶ 83 (alleging that "Quantum Metric also uses Kaiser Plan Members' communications for its own research and analysis purposes").

Plaintiffs maintain that they and others similarly situated did not consent to the interception of their information by the third parties. Plaintiffs also contend that Kaiser allowed the interception even though it was required to protect that information under, *e.g.*, HIPAA. *See* FAC ¶ 7; *see also* 42 U.S.C. § 1320d-6 (providing for a criminal penalty if a person knowingly, *e.g.*, "discloses individually identifiable health information to another person"); 45 C.F.R. § 164.508(a)(1) (providing that, as a general rule, "a covered entity may not use or disclose protected health information without an authorization that is valid under this section").

Based on the above as well as other allegations, Plaintiffs bring the following class claims (some on behalf of a multistate class and some on behalf of a subclass(es)[3]):

(1) Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*

(2) Violation of the California Invasion of Privacy Act, Cal. Pen. Code § 631.

(3) Common law invasion of privacy – intrusion upon seclusion.

(4) Invasion of privacy and violation of the California Constitution, Art. I, § 1.

(5) Breach of express contract.

(6) Breach of implied contract.

(7) Negligence per se.

(8) Violation of the California Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

(9) Violation of the California Confidentiality of Medical Information Act, Cal.

[3] The multistate class is defined as "[a]ll Kaiser Plan Members in the Kaiser Operating States who used the Kaiser Permanente website or mobile applications." FAC ¶ 251.

Civ. Code § 56.10.

(10) Statutory larceny, Cal. Pen. Code §§ 484, 496.

(11) Violation of the District of Columbia Consumer Protection Procedures Act, D.C. Code § 28-3901, *et seq.* (brought by Jane Doe II only).

(12) Violation of the Georgia Uniform Deceptive Trade Practices Act, Ga. Code Ann. § 10-1-370 *et seq.* (brought by John Doe II only).

(13) Violation of the Georgia Computer Systems Protection Act, Ga. Code Ann. § 16-9-93. (brought by John Doe II only).

(14) Violation of the Georgia Insurance and Information Privacy Protection Act, Ga. Code Ann. § 33-39-1 *et seq.* (brought by John Doe II only).

(15) Violation of the Maryland Wiretapping and Electronic Surveillance Act, Md. Code Ann., Cts. & Jud. Proc. § 10-401 *et seq.* (brought by Jane Doe III only).

(16) Violation of the Oregon Unlawful Trade Practices Act, Or. Rev. Stat. § 646.605 *et seq.* (brought by Jane Doe V only),

(17) Violation of the Virginia Computer Crimes Act, Va. Code Ann. § 18.2152.1 *et seq.* (brought by Jane Doe IV only).

(18) Violation of the Virginia Insurance Information and Privacy Protection Act, Va. Code Ann. § 38.2-600 *et seq.* (brought by Jane Doe IV only).

(19) Violation of the Washington Consumer Protection Act, Wash. Rev. Code § 19.86 *et seq.* (brought by Jane Doe only).

(20) Violation of the Washington Privacy Act, Wa. Rev. Code § 9.73 *et seq.* (brought by Jane Doe only).

(21) Violation of the Washington Health Care Information Act, Wash. Rev. Code § 70.02.005 *et seq.* (brought by Jane Doe only).

Kaiser has challenged all of Plaintiffs' claims, arguing that some of the Plaintiffs lack standing to proceed with suit and that all of the claims should be dismissed for failure to state a claim for relief.

II. STANDING

A. Legal Standard

A motion to dismiss for lack of subject matter jurisdiction – including lack of standing – is brought under Federal Rule of Civil Procedure 12(b)(1). *See In re Apple iPhone Antitrust Litig.*, 846 F.3d 313, 319 (9th Cir. 2017) (stating that "[a] Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction, including for failure to allege injury sufficient for Article III standing, may be made at any time").

> A Rule 12(b)(1) jurisdictional attack may be facial or factual. In a facial attack, the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction. By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction. . . .

Safe Air For Everyone v. Meyer, 373 F.3d 1035, 1039 (9th Cir. 2004).

B. John Doe II and Jane Does II-V

In the case at bar, Kaiser makes only a facial challenge, not a factual one, to standing – specifically, to the standing of John Doe II and Jane Does II-V (five out of the seven Plaintiffs).

For standing, a plaintiff must show that they have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016); *see also TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). With respect to the first element, an injury in fact must be concrete, *i.e.*, real and not abstract. *See id.* at 2204; *see also Spokeo*, 578 U.S. at 339 ("To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'").

According to Kaiser, there are insufficient allegations on standing with respect to John Doe II and Jane Does II-V because there are no clear allegations that they submitted personal information to Kaiser and/or that their personal information was disclosed to any of the third parties at issue. Kaiser asserts that, "[i]nstead of pleading any facts regarding the interception of their personal information, the New Does attempt to piggyback onto John Doe I and Jane Doe I's

allegations, alleging only that their identified information was 'similarly intercepted' by each of the Vendors in the manner described for John Doe I and Jane Doe I." Mot. at 6.

Kaiser is correct that the specific examples contained in the FAC are about John Doe and Jane Doe only (whether the third party involved is, *e.g.*, Quantum Metric, Adobe, Bing, Google, or Twitter). *See, e.g.*, FAC ¶ 86 (making allegations about Jane Doe logging into the patient portal on 5/31/2023 and her information being intercepted by Quantum Metric); FAC ¶ 88 (making allegations about John Doe logging into the patient portal on 6/5/2023 and his information being intercepted by Quantum Metric). The FAC then contains more generalized allegations that the other Plaintiffs, as well as other Class members, had similar experiences. *See, e.g.*, FAC ¶ 87 (alleging that Kaiser "similarly allowed Quantum Metric to intercept log-in information for [the remaining Plaintiffs] and other members of the Classes"); FAC ¶ 97 (alleging that when John Doe II and Jane Does II-V "accessed the Kaiser Permanente website and Patient Portal, their communications were similarly intercepted by Quantum Metric").

The Court rejects Kaiser's position that this means John Doe II and Jane Does II-V lack standing. It is plausibly alleged that, so long as the other Plaintiffs used the website and mobile applications, their information was treated similarly as John Doe's and Jane Doe's. In other words, it may reasonably be inferred that the same policies or practices applied to all Kaiser plan members. Certainly there is nothing to suggest that John Doe and Jane Doe were subject to unique treatment. Here, Plaintiffs have alleged that all of them did regularly use the website and mobile applications. For instance, the following allegation is made for John Doe:

> Plaintiff John Doe regularly uses Kaiser Permanente's website, Patient Portal, and mobile application to access medical information and communicate with his health care providers, including making appointments, reviewing and ordering prescriptions, researching providers and medical conditions, communicating with providers, checking medical results, and reviewing his medical history.

FAC ¶ 15. The same allegation is repeated for each of the remaining Plaintiffs. *See* FAC ¶ 19 (John Doe II); FAC ¶ 23 (Jane Doe); FAC ¶ 27 (Jane Doe II); FAC ¶ 31 (Jane Doe III); FAC ¶ 35 (Jane Doe IV); FAC ¶ 39 (Jane Doe V).

Accordingly, the Court holds that John Doe II and Jane Does II-V have sufficiently alleged

standing. To the extent *Cousin v. Sharp Healthcare*, No. 22-CV-2040, 2023 WL 4484441 (S.D. Cal. July 12, 2023), reaches a contrary conclusion, the Court respectfully declines to follow it.

III. FAILURE TO STATE A CLAIM FOR RELIEF

A. Legal Standard

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court's decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), a plaintiff's "factual allegations [in the complaint] 'must . . . suggest that the claim has at least a plausible chance of success.'" *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135 (9th Cir. 2014). The court "accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party." *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But "allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively." *Levitt*, 765 F.3d at 1135 (internal quotation marks omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. "The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.* (internal quotation marks omitted).

B. Group Pleading

As an initial matter, Kaiser notes that Plaintiffs have sued three Kaiser entities: KFHP, Hospitals, and TPMG. Kaiser argues that the claims against two of the entities – Hospitals and TPMG (*i.e.*, the health care providers) – should be dismissed pursuant to Rule 12(b)(6) because Plaintiffs have not alleged any wrongdoing on their part and instead have engaged in impermissible group pleading (*i.e.*, lumping all Defendants together).

Kaiser's argument has merit. Plaintiffs have alleged in conclusory terms only that all

Kaiser entities have a hand in the operation of the website and mobile applications. But the documents attached to the FAC indicate that the website and mobile applications at issue are owned and operated by KFHP only. *See, e.g.*, FAC, Ex. 2 (Privacy Statement at 1) (stating that "the Site . . . is owned and operated by Kaiser Foundation Health Plan, Inc."). This provides a basis for suit against KPHP, but there is no indication that the health care providers (Hospitals and TPMG) had anything to do with how the website and mobile applications are run, even if Kaiser plan members engaged in communications with their health care providers through the website and mobile applications.

Plaintiffs contend: "Plaintiffs' claims here involve the interception of communications between Plaintiffs and their health care providers on the Site and Apps and each Defendant is fully aware of its role in that process." Opp'n at 11. But that argument does not identify how the health care providers specifically have engaged in any wrongdoing. There is also nothing to suggest that the health care providers have the same exact role vis-à-vis the website and mobile applications that KFHP does. *Cf. United States ex rel. Silingo v. Wellpoint, Inc.*, 904 F.3d 667, 677 (9th Cir. 2018) (stating that "a complaint need not distinguish between defendants that had the exact same role in a fraud"; "'[t]here is no flaw in a pleading . . . where collective allegations are used to describe the actions of multiple defendants who are alleged to have engaged in precisely the same conduct'"). Thus, Plaintiffs' reliance on this Court's decision in *United States ex rel. Osinek v. Permanente*, No. No. 13-cv-03891-EMC, 2023 U.S. Dist. LEXIS 104693, *52 (in False Claims Act case, citing *Silingo*), is unavailing.

The Court, therefore, grants the motion to dismiss Hospitals and TPMG from the case but with leave to amend. If Plaintiffs do amend to assert claims against Hospitals and TPMG, Plaintiffs must have a good faith basis, consistent with their Rule 11 obligations, to allege that Hospitals and TPMG engaged in wrongdoing vis-à-vis the operation of the website and mobile applications. The Court also gives Plaintiffs the option of not amending now but rather seeking leave to amend should, *e.g.*, discovery reveal that Hospitals and/or TPMG played a role that would support liability.

C. Consent

Kaiser argues next that all of Plaintiffs' claims fail because consent is a defense to all of the claims and Plaintiffs consented to Kaiser's alleged conduct (namely, allowing third parties to intercept information) when they agreed to the TAC for the website and mobile applications and the related Privacy Statement.

As a preliminary matter, Kaiser does not seem to dispute Plaintiffs' contention that consent is an affirmative defense – *i.e.*, an issue to be proven by a defendant and not a plaintiff. *See, e.g.*, *Doe v. Meta Platforms, Inc.*, No. 22-cv-03580-WHO, 2023 U.S. Dist. LEXIS 158683, at *14 (N.D. Cal. Sept. 7, 2023) (addressing the issue of consent under the federal Electronic Communications Privacy Act). However, a complaint may still be subject to dismissal under Rule 12(b)(6) based on an affirmative defense so long as the "affirmative defense . . . appears on [the] face [of the complaint]." *El-Shaddai v. Zamora*, 833 F.3d 1036, 1044 (9th Cir. 2016). Kaiser asserts that that is the case here.

Plaintiffs' primary argument on consent is that anything less than written consent from a Kaiser plan member is invalid and that was not done here (*i.e.*, because all that Kaiser did was provide the TAC and related Privacy Statement). Plaintiffs rely on HIPAA in support of their position. *See* 45 C.F.R. § 164.508(a)(1) (providing that, as a general matter, "a covered entity may not use or disclose protected health information without an authorization that is valid under this section"); *id.* § 164.508(c)(1) (addressing the "core elements" of a valid authorization which includes, *inter alia*, "[a] description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion," "to whom the covered entity may make the requested use or disclosure," "[a] description of each purpose of the requested disclosure," and "[s]ignature of the individual and date"). The problem for Plaintiffs is that they have not shown that the HIPAA standard on consent applies to each of the claims that has been asserted in the FAC.

On the other hand, as Plaintiffs contend, there seem to be factual questions related to consent, including how a reasonable person would construe the statements made by Kaiser in its Privacy Statement. *Cf. Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1063 (N.D. Cal. 2021)

(stating that, "if a reasonable . . . user could have plausibly interpreted the contract language as not disclosing that [the defendant] would engage in particular conduct, then [the defendant] cannot obtain dismissal of a claim about that conduct (at least not based on the issue of consent)"). Kaiser has not shown at this juncture that all Kaiser members consented to the alleged interception of the breadth of information at issue.

In light of these consideration, the Court does not, at this juncture, make a blanket ruling on consent that covers all claims asserted by Plaintiffs in the FAC. This is without prejudice to the Court entertaining the issue of consent at a later juncture.

D. Liability Theories

For the remainder of its motion to dismiss, Kaiser makes arguments that are specific to each of the twenty-one causes of action alleged in Plaintiffs' operative complaint. However, before addressing these specific arguments, the Court finds it helpful to separate out Plaintiffs' factual theories in support of liability.

Plaintiffs have essentially asserted two different factual scenarios supporting liability: (1) Kaiser used third parties to collect and/or use information for the benefit of Kaiser (essentially, hiring third parties as vendors); and (2) Kaiser allowed third parties to collect and/or use information for the benefit of the third parties themselves (essentially, selling or otherwise giving information to third parties).

As an initial matter, the Court notes that the FAC does not always make clear which third parties fell into which category above. (The Court recognizes that a third party could theoretically fall into both categories.) This is a significant problem. Although Plaintiffs has made many allegations specific to the various third parties, Plaintiffs do not clearly differentiate among the third parties with respect to the categories above.

Putting aside this problem, the Court has a more fundamental concern with the factual scenario described in (2) above. Even if Plaintiffs sufficiently alleged that all six of the third parties collected and/or used information about Kaiser plan members for the third parties' own benefit, Plaintiffs have not alleged that the third parties did so with the knowledge and/or approval of Kaiser. In other words, as the FAC is currently pled, Kaiser simply hired the third parties to do

work for Kaiser, which exposed the third parties to personal information about members, but there is no indication that Kaiser then signed off (either explicitly or implicitly) on the third parties taking that information and using it for their own purposes (and not solely for Kaiser's use). In fact, if anything, the Privacy Statement suggests that Kaiser took some steps to guard against such conduct on the part of third parties. *See* FAC, Ex. 2 (Priv. St. § 13) ("Information disclosed to vendors or contractors for operational purposes may not be re-disclosed to others by such a vendor or contract, except as permitted by [Kaiser] and applicable law.").

Accordingly, to the extent Plaintiffs have pled claims based on the factual scenario in (2), the Court dismisses all such claims as there is no alleged wrongdoing by Kaiser – *i.e.*, that Kaiser knew and/or approved of third parties collecting and/or using information for their own purposes. Indeed, there is not even an allegation that Kaiser negligently failed to take steps to ensure that third parties could not collect and/or use information for their own benefit. Thus, the remainder of this order addresses Plaintiffs' claims as based on the factual scenario in (1) – *i.e.*, that Kaiser hired third parties to collect and/or use information for the benefit of Kaiser.

E. Count 1: Claim for Violation of the Electronic Communications Privacy Act

In Count 1, Plaintiffs bring a multistate class claim based on the federal Electronic Communications Privacy Act ("ECPA"). *See* FAC ¶ 265 (alleging that the claim is asserted by Plaintiffs individually and on behalf of the Kaiser Operating States Class). The ECPA provides for liability where a person, *e.g.*,

- "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication";
- "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection"; and
- "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in

violation of this subsection."

18 U.S.C. § 2511(1)(a), (c), (d).

However, the ECPA also provides that it is not unlawful

> for a person not acting under color of law to intercept a wire, oral, or electronic communication [1] where such person is a party to the communication or [2] where one of the parties to the communication has given prior consent to such interception *unless* such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id. § 2511(2)(d) (emphasis added).

In the instant case, Kaiser argues that Plaintiffs have failed to state an ECPA claim because (1) Kaiser was clearly a party to the communications at issue (*i.e.*, communications between Kaiser plan members and Kaiser made through the website or mobile applications) and (2) Kaiser – a party to the communications – gave consent to the interception by the third parties (which was done for Kaiser's benefit). In response, Plaintiffs do not dispute either (1) or (2) and instead argue that they have a viable ECPA claim based on the "crime-tort exception" delineated in the statute. Thus, the issue for the Court is whether Kaiser had third parties intercept communications between itself and its plan members "for the purpose of committing [a] criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

In addressing this issue, the Court begins with *Sussman v. ABC*, 186 F.3d 1200 (9th Cir. 1999), one of the main Ninth Circuit cases addressing the crime-tort exception in the ECPA. In *Sussman*, the television network ABC hired a person to pose as a psychic telephone adviser so as to gain access to a company called the Psychic Marketing Group ("PMG"). The person hired by ABC used surveillance devices to record activities at PMG. Subsequently, PMG employees filed a suit against ABC, alleging eavesdropping under the ECPA.

The Ninth Circuit was asked to consider whether the crime-tort exception in § 2511(2)(d) applied. It noted first that ABC was not automatically exempt just because there was a

> lawful purpose for the surreptitious taping, namely news gathering. . . . [T]he existence of a lawful purpose does not mean that the interception is not also for a tortious or unlawful purpose. For example, assume that a news gathering organization secretly videotapes bedroom activities. Even though there may be a

> legitimate news gathering purpose (e.g., listening for "pillow talk" about some newsworthy event), public airing of such a tape may be illegal or tortious under state law. Under these circumstances, the taping could be for both a legitimate purpose (news gathering) and also an unlawful or tortious purpose (airing private intimate conduct). The existence of the lawful purpose would not sanitize a tape that was also made for an illegitimate purpose; the taping would violate section 2511.

Id. at 1202.

That being said, the Ninth Circuit went on to note that "[p]laintiffs here have pointed to no state statute or caselaw indicating that it was tortious or illegal for ABC to air the tapings made by [the hired individual]." *Id.*

> While plaintiffs have claimed that ABC's story was factually incorrect and unfair, they have never claimed it was not newsworthy. Nor do they argue that the tape was made for the purpose of committing some other subsequent crime or tort. Rather, plaintiffs point to Sanders and argue that the taping itself was tortious. If an otherwise lawful taping violates section 2511 when committed for a prohibited purpose, argue plaintiffs, the section must also be violated when the taping itself is illegal or tortious. *This argument finds no support in the statute. Under section 2511, "the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception – its intended use – was criminal or tortious." Payne v. Norwest Corp.*, 911 F. Supp. 1299, 1304 (D. Mont. 1995*), aff'd in part and rev'd in part*, 113 F.3d 1079 (9th Cir. 1997). *See also Deteresa v. American Broad. Cos.*, 121 F.3d 460, 467 n.4 (9th Cir. 1997) (emphasizing the distinction between a taping that is itself tortious or criminal, and one carried out *for the purpose of committing some other crime or tort*). Where the taping is legal, but is done for the purpose of facilitating *some further impropriety*, such as blackmail, section 2511 applies. Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere.

Id. at 1202-03 (emphasis added). In short, the "criminal or tortious purpose must be separate and independent from the act of the recording [*i.e.*, the act of interception]." *Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022).

Other circuit courts have adopted the same approach. *See Caro v. Weintraub*, 618 F.3d 94, 98 (2d Cir. 2010) ("Several of our sister circuits [including the Ninth Circuit in *Sussman*] have tackled the issue, each reaching the conclusion that . . . the defendant must have the intent to use the illicit recording to commit a tort [or] crime *beyond* the act of recording itself.") (emphasis added). In *Caro*, the Second Circuit underscored:

> There is a temporal thread that runs through the fabric of the statute

> and the case law. At the time of the recording the offender must intend to use the recording to commit a criminal or tortious act. Merely intending to record the plaintiff is not enough. If, at the moment he hits "record," the offender does not intend to use the recording for criminal or tortious purposes, there is no violation. But if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation, a civil cause of action exists under the Wiretap Act [*i.e.*, the ECPA].
>
> Intent may not be inferred simply by demonstrating that the intentional act of recording itself constituted a tort. A simultaneous tort arising from the act of recording itself is insufficient. Congress chose the word "purpose" for a reason. Therefore, the offender must have as her objective a tortious or criminal result. Had Congress intended for the act of recording itself to provide the tortious intent necessary, it could have chosen to define the exception in terms of interception of oral communications *resulting* in a tortious or criminal act. But Congress limited the cause of action to instances where one party to the conversation deliberately seeks to harm the other participant through the information intercepted.

Id. at 99-100 (emphasis in original).

Given the parameters laid out above, Plaintiffs have failed to plead the crime-tort exception. According to Plaintiffs, "Kaiser remains liable because the communications were intercepted [1] for the purpose of violating HIPAA, a criminal act, and [2] to tortiously collect personal information without consent or compensation to obtain market research and consumer analysis without paying for it." Opp'n at 15. But both of these arguments are problematic.

In the first argument, Plaintiffs point to a violation of HIPAA because Kaiser knowingly disclosed individually identifiable health information to third parties without authorization (*i.e.*, by allowing third parties to intercept communications). *See* Opp'n at 16. But this argument is contrary to *Sussman* which holds that the act of interception itself cannot be the crime or the tort. Violation of HIPAA was not the purpose of the alleged interception.

As to the second argument, the tort identified by Plaintiffs is the collection of personal information (without consent or compensation). But again that inheres in the alleged interception. The collection of information itself was not for the purpose of committing a crime or tort (at least, as pled); rather, the apparent purpose was to use the information collected for market research and consumer analysis solely for the benefit of Kaiser in better reaching and serving its patients. *Cf. In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797 (N.D. Cal. 2022) ("Multiple courts in this district have found that the crime-tort exception . . . is inapplicable where the defendant's

primary motivation was to make money, not to injure plaintiffs tortiously."). *In re Toys R Us, Inc. Privacy Litigation*, No. C 00-2746 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001), is distinguishable; the court did not address the issue of whether the website owner – who allowed another company to intercept the plaintiffs' communications with the websites – had a tortious purpose. Rather the issue in *Toys R Us* was whether the party who intercepted the communications had a tortious purpose. *See id.* at *26 (finding that plaintiffs' "allegations are sufficient to allege that Coremetrics [*i.e.*, not Toys R Us who owned the websites at issue] intercepted plaintiffs' electronic communications for such tortious purposes as 'spying' on plaintiffs' private Websurfing activities and/or to essentially steal from plaintiffs information for which Coremetrics would otherwise have to pay plaintiffs"). Plaintiffs have not sufficiently alleged a tortious purpose in Kaiser's collection of information.

Accordingly, as pled, the ECPA claim does not plausibly state a basis for liability. The claim is dismissed with leave to amend.

F. Count 2: Claim for Violation of the California Invasion of Privacy Act

In Count 2, Plaintiffs bring a claim for violation of the California Invasion of Privacy Act ("CIPA"), which is similar in nature to the ECPA. *See In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 797 (N.D. Cal. 2022) (noting that CIPA "mirrors" the ECPA "with a few important exceptions"). The claim is brought as a multistate class claim (*i.e.*, on behalf the Kaiser Operating States Class). Alternatively, Plaintiffs assert the claim on behalf of a California subclass.

Under CIPA,

> [a]ny person who, **[1]** by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who **[2]** willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who **[3]** uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who **[4]** aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or

> cause to be done any of the acts or things mentioned above in this section, is punishable . . . .

Cal. Pen. Code § 631(a) (emphasis added).

1. Choice of Law

In a previous order, the Court compelled John Doe, the only California Plaintiff, to arbitration. As a result of that ruling, the first issue the Court must address is choice of law, *i.e.*, whether CIPA (a California law) can apply to all Plaintiffs and all putative class members regardless of their residence.

Plaintiffs contend that California law applies across the board to all Kaiser plan members because the TAC for use of the website and mobile applications provide that they are "GOVERNED BY CALIFORNIA LAW WITHOUT REGARD TO ITS PRINCIPLES OF CONFLICTS OF LAW." FAC, Ex. 1 (TAC at 12). However, as Kaiser points out, the Ninth Circuit has explained that,

> [i]f a state law does *not* have limitations on its geographical scope, courts will apply it to a contract governed by that state's law, even if parts of the contract are performed outside of the state. When a law *contains* geographical limitations on its application, however, courts will not apply it to parties falling outside those limitations, *even if* the parties stipulate that the law should apply.

Gravquick A/S v. Trimble Navigation Int'l, 323 F.3d 1219, 1223 (9th Cir. 2003) (emphasis added); *see also O'Connor v. Uber Techs., Inc.*, 58 F. Supp. 3d 989, 1004 (N.D. Cal. 2014) (noting that, in *Gravquick*, the Ninth Circuit "recognized that parties' agreement to apply California law must yield in those circumstances where the law in question contains 'geographical limitations'"); *Cotter v. Lyft, Inc.*, 60 F. Supp. 3d 1059, 1065 (N.D. Cal. 2014) (noting that, "[e]ven if [a] choice of law provision were intended to confer upon out-of-state drivers a cause of action for violation of California's wage and hour laws, it could not do so" because "[a]n employee cannot create by contract a cause of action that California law does not provide" – *i.e.*, because California wage-and-hour law contains a geographical limitation; citing *Gravquick*).[4]

[4] In *Gravquick*, the Ninth Circuit noted that,

> [a]lthough the California legislature undoubtedly was primarily concerned with protecting California dealers, the [California

Here, CIPA does contain express geographical limitations. *See* Cal. Pen. Code § 631 (providing for liability where a person "willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received *at any place within this state*") (emphasis added). In addition, there is a presumption against extraterritoriality under California law. *See Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1207 (2011) (referring to the "so-called presumption against extraterritorial application[;] [h]owever far the Legislature's power may theoretically extend, we presume the Legislature did not intend a statute to be operative, with respect to occurrences outside the state, . . . unless such intention is clearly expressed or reasonably to be inferred from the language of the act or from its purpose, subject matter or history") (internal quotation marks omitted). In light of the above, the provision in the TAC on which Plaintiffs rely has no force.

The Court therefore applies California choice-of-law rules to determine which state's law should actually govern. *See Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 589 (9th Cir. 2012) ("'A federal court sitting in diversity must look to the forum state's choice of law rules to determine the controlling substantive law.'").

> Under California's choice of law rules, the class action proponent bears the initial burden to show that California has "significant contact or significant aggregation of contacts" to the claims of each class member. Such a showing is necessary to ensure that application of California law is constitutional. Once the class action proponent makes this showing, the burden shifts to the other side to demonstrate "that foreign law, rather than California law, should apply to class claims."

Id. at 589-90.

> Equipment Dealers Act] includes no express requirement limiting its protection to dealers located in California. Therefore, the CEDA can be applied to an out-of-state dealer through a choice of law provision in a contract. Because both parties agree that California law governs the [International Distributor Agreement], the CEDA applies to this transaction.

Gravquick, 323 F.3d at 1223.

For purposes of this opinion, the Court assumes that California has significant contact relative to all Plaintiffs and class members' wiretapping claims because Kaiser, which allegedly aided and abetted the third parties' interception, is based in California.

The question therefore is whether Kaiser has shown that foreign law and not California law should apply – *i.e.*, that the interests of other states outweigh California's interest in having its own law applied. *See id.* at 590 ("California law may only be used on a classwide basis if 'the interests of other states are not found to outweigh California's interest in having its law applied.'"). To determine whether the interests of other states outweigh California's interest, the Court must apply a three-step governmental interest test.

> First, the court determines whether the relevant law of each of the potentially affected jurisdictions with regard to the particular issue in question is the same or different.
>
> Second, if there is a difference, the court examines each jurisdiction's interest in the application of its own law under the circumstances of the particular case to determine whether a true conflict exists.
>
> Third, if the court finds that there is a true conflict, it carefully evaluates and compares the nature and strength of the interest of each jurisdiction in the application of its own law to determine which state's interest would be more impaired if its policy were subordinated to the policy of the other state, and then ultimately applies the law of the state whose interest would be more impaired if its law were not applied.

Id.

At step one,

> "there are material differences between CIPA and the wiretapping statutes of the other 49 states [which includes the Kaiser Operating States]. For example, some states expressly exclude email from their wiretapping statutes, others require only single party consent, and still others require plaintiffs to prove that they had either an objective or subjective expectation of privacy. These differences are material, as their application would 'spell the difference between the success and failure of a claim.' Moreover, there are also 'material differences in the remedies given by state laws,' as some states provide for injunctive relief while others do not, and the states vary as to whether damages may be recovered."

James v. Walt Disney Co., No. 23-cv-02500 EMC, 2023 U.S. Dist. LEXIS 200997, at *49-50 (N.D. Cal. Nov. 8, 2023) (quoting *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 602-03 (N.D. Cal.

2015)).

At step two, a true conflict exists because each of the implicated jurisdictions in the instant case has an interest in the application of its own law. "'[E]very state has an interest in having its law applied to its resident claimants,'" *i.e.*, to protect its residents' privacy interests, and "states may permissibly differ on the extent to which they will tolerate a degree of lessened protection for consumers to create a more favorable business climate for the companies that the state seeks to attract to do business in the state." *Mazza*, 666 F.3d at 591-92.

Finally, at step three, "if California law were applied to the entire class, foreign states would be impaired in their ability to calibrate liability to foster commerce." *Id.* at 593. California does not have a predominant interest simply because Kaiser is based in California and allegedly aided and abetted third parties from the state. Because wiretapping statutes are designed to protect the privacy interests of individual members, the residences of the individuals are more important to the respective sovereign than the residence of the alleged wrongdoer.[5]

Accordingly, the Court finds that, under a choice-of-law analysis, CIPA does not apply across the board to all Plaintiffs and class members' wiretapping claims. Rather, the wiretapping law that applies turns on the residence of the Kaiser plan member. That means that only a California Plaintiff can bring a CIPA claim. Because the Court has compelled John Doe, the only

---

[5] Based on the Court's analysis above, it need not engage in an analysis of where is the "place of wrong" for purposes of the case at bar. *See Mazza*, 666 F.3d at 593 (considering the place of wrong at step three – *i.e.*, in evaluating which state's interest would be most impaired if its policy were subordinated to the policy of another state). Under California law, the place of wrong has the predominant interest, and the place of wrong is "the state where the last event necessary to make the actor liable occurred." *Id.*

While the Court does not make any rulings on the place of wrong, there is a fair argument that the last event necessary to make Kaiser liable (even as simply an aider and abettor) was when a third party actually intercepted the communications at issue. In their papers, Plaintiffs seem to have conceded that interceptions take place where a Kaiser plan member resides. *See* Opp'n at 35 (asserting that Jane Doe III does not seek extraterritorial application of a Maryland statute because "she has alleged that her communications were intercepted or disclosed when sent from or received in Maryland" where she resides); *cf. Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 130-31 (3d Cir. 2022) (in discussing Pennsylvania's wiretapping statute, stating that "[e]lectronic communications are . . . 'intercepted' when software reroutes communications to an interceptor"; thus, "NaviStone intercepted Popa's communications at the point where it routed those communications to its own servers[,] [a]nd that was at Popa's browser, not where the signals were received at NaviStone's servers").

California Plaintiff to arbitration, there is no Plaintiff who has standing to assert a CIPA claim. The CIPA claim is therefore dismissed, although with leave to amend.

2. Kaiser's Remaining Arguments

Based on the Court's ruling above, it need not address Kaiser's remaining arguments that (1) it cannot be held liable when all that it did was use the third parties as a tool and (2) Plaintiffs have failed to plead that an interception took place while communications were in transit between a Kaiser plan member and Kaiser.

But as it seems likely that Plaintiffs will be able to find a new California Plaintiff to add to the case, the Court finds it worthwhile to provide some comments on the first argument in particular.

As discussed at the hearing, courts have reached differing conclusions as to whether a party to a communication – who ordinarily would not be liable for a CIPA violation since it cannot "intercept" a communication to which it is a party – can be held liable if the party hires a third party to do work for the party's own benefit.[6] Many of these courts have looked to two state court cases in reaching their conclusions: *Rogers v. Ulrich*, 52 Cal. App. 3d 894 (1975), and *Ribas v. Clark*, 38 Cal. 3d 355 (1985).

In *Rogers*, the plaintiff sued the City of San Jose and a city employee because the latter had recorded portions of a conversation he had with the plaintiff. Although CIPA includes a provision on the recording of confidential communications, *see* Cal. Pen. Code § 632(a) (providing for punishment where a person "intentionally and without the consent of all parties to a confidential communication[] uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication"), the only CIPA provision at issue in *Rogers* was § 631 (which focuses on wiretapping). *See Rogers*, 52 Cal. App. 3d at 899 (addressing plaintiff's request to amend to allege a violation of § 632). The appellate court upheld the trial court's order granting the defendants' motion for judgment on the § 631 claim.

[6] In *James*, 2023 U.S. Dist. LEXIS 200997, the Court was not presented with this issue because it was never raised by the defendant. *See id.* at *22 n.3 ("Disney makes no argument that it cannot be held liable because all that Disney did was hire a third party to engage in conduct that Disney could have lawfully done itself.").

> The question is whether the statute covers the recording of a conversation made by a participant rather than by a third party. [ ] The statute prohibits three ways of obtaining information being sent over a telephone or telegraph line: (1) tapping the line, (2) making an unauthorized connection with the line, and (3) reading, attempting to read, or learning the contents or meaning of a message while the message is in transit. As to the third method, a recording made by a participant does not intercept the message while it is in transit; the recording rather transcribes the message as it is being received. As to the first two methods, the key phrases, "taps" and "makes any unauthorized connection," are vague and nowhere defined. However, Penal Code section 630 is a declaration of legislative finding and intent; it speaks of preventing eavesdropping and other invasions of privacy, thus suggesting that participant recording was not meant to be included. "Eavesdropping" is the problem the Legislature meant to deal with; "eavesdrop" is defined in Webster's Seventh New Collegiate Dictionary (1972) as "to listen secretly to what is said in private." It is never a secret to one party to a conversation that the other party is listening to the conversation; only a third party can listen secretly to a private conversation. The trial court was right in determining that appellant's evidence did not make out a case under the statute.

Id. at 898-99.

In *Ribas*, the plaintiff and his wife were engaged in divorce proceedings. After the plaintiff had a heated phone call with the wife's lawyer, the wife visited a friend and used the phone to call the plaintiff. The wife asked the friend to listen in on the call on an extension telephone. During the conversation, the plaintiff told his wife about the discussion he had with her lawyer. *See Ribas*, 38 Cal. 3d at 358. The plaintiff later sued the friend because she had listened in on the conversation. He alleged a violation of, *inter alia*, § 631. The California Supreme Court agreed with the plaintiff that he had a viable § 631 claim. "Section 631 was aimed at one aspect of the privacy problem – eavesdropping, or the secret monitoring of conversations by third parties." *Id.* at 359 (citing *Rogers*). It prohibited "far more than [just] illicit wiretapping," extending as well to the "simultaneous dissemination to an unannounced second auditor. [¶] As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication – the right to control the nature and extent of the firsthand dissemination of his statements." *Id.* at 360-61 (distinguishing "the secondhand repetition of the contents of a conversation"). The court added: "[I]t is probable that the Legislature viewed section 631 as a means of proscribing attempts to circumvent other aspects of the Privacy Act, e.g., by requesting a

secretary to secretly transcribe a conversation over an extension, rather than tape recording it in violation of section 632." *Id.* at 361.

As indicated above, courts have often asked whether the cases before them were more similar to *Rogers* or *Ribas*.

For example, in *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823 (N.D. Cal. 2021) (Beeler, J.), the defendants were (1) Noom, which operated a web application helping users lose weight and lead healthier websites, and (2) FullStory, a software provider. Noom used FullStory's software – called "session replay" – to record what visitors to the Noom website were doing, as this would purportedly improve website design and the user experience. The plaintiffs were users of the Noom website. They claimed that FullStory violated § 631 by intercepting their communications with Noom, and Noom by aiding and abetting FullStory. *See Graham*, 533 F. Supp. 3d at 827-28, 831.

Judge Beeler rejected the plaintiffs' position. She began by noting that, in a different case (*Moosejaw*), Judge Chhabria held that the plaintiffs – who articulated a similar theory – had plausibly pleaded a § 631 claim. But she found *Moosejaw* and other cases distinguishable because the data collected was not sold to third parties but used solely for the website host.

> In *Moosejaw*, . . . NaviStone was a marketing company that partnered with e-commerce sites to intercept visitor data and create marketing databases of consumer information. In *Facebook*, Facebook tracked its users to third-party websites (through Facebook's code on the websites) – even when its users were not signed into Facebook, and then it sold that data to advertisers. NaviStone and Facebook were independent parties who mined information from other websites *and sold it*: NaviStone through its code on participating e-commerce sites and Facebook through its plug-ins on third-party sites.
>
> By contrast, FullStory is a vendor that provides a software service that captures its clients' data, hosts it on FullStory's servers, and allows the clients to analyze their data. Unlike NaviStone's and Facebook's aggregation of data for resale, there are no allegations here that FullStory intercepted *and used the data itself. Instead, as a service provider, FullStory is an extension of Noom. It provides a tool – like the tape recorder in* Rogers – that allows Noom to record and analyze its own data in aid of Noom's business. It is not a third-party eavesdropper.

Id. at 832-33 (emphasis added).

In *Williams v. What If Holdings, LLC*, No. C 22-03780 WHA, 2022 U.S. Dist. LEXIS 230732, (N.D. Cal. Dec. 22, 2022), Judge Alsup addressed a similar case and reached the same conclusion as did Judge Beeler. The defendants in the case were What If, the owner and operator of a website, and ActiveProspect, a software provider. What If used ActiveProspect's software to record, *e.g.*, a website user's keystrokes and clicks. The plaintiff sued both the defendants for a violation of § 631. Her claim against What If was based on prong (4) of § 631 – *i.e.*, that it had aided and abetted ActiveProspect's eavesdropping. In contrast, her claim against ActiveProspect was based on prong (2) of § 631 – *i.e.*, that it had read the contents of a communication while in transit.

Judge Alsup noted that,

> [b]ecause a party to the communication is exempt from liability under CIPA, our dispositive question is whether ActiveProspect constitutes a third-party eavesdropper. Put differently, the question boils down to whether ActiveProspect was an independent third party hired to eavesdrop on What If's communications, or whether ActiveProspect's software was merely a tool that What If used to record its own communications with plaintiff.
>
> Our facts suggest the latter. The complaint most pertinently alleges that What If deployed ActiveProspect's TrustedForm recording software only on What If's websites and that the recordings were stored and accessed on ActiveProspect's servers. These limited allegations are not enough to show that ActiveProspect was a third-party eavesdropper as contemplated by Section 631(a).

Id. at *7.

Addressing the plaintiff's concern that a website owner could circumvent § 631 by hiring a vendor to record communications, Judge Alsup pointed out that that would not be the case:

> Our relevant inquiry here is whether a website owner's usage of third-party recordation software can be considered equivalent to having hired a third party to record. That inquiry thus determines whether or not the software provider can be considered a third party in the first place for purposes of a Section 631(a) analysis. Judge Laurel Beeler's reasoning in deciding a series of factually similar cases is instructive: a key distinction is whether or not the alleged third-party software provider *aggregates or otherwise processes the recorded information, which might suggest that the software vendor independently "uses" the gathered data in some way*.

Id. at *7-8 (emphasis added). "Just like in *Graham*, there are no facts here to suggest that

ActiveProspect 'intercepted and used the data itself.'" *Id.* at *8; *see also id.* at *9 (stating that the recordation was "qualitatively different from data mining"). Judge Alsup distinguished authorities cited by the plaintiff, noting that the recordation in those cases was "much broader [in] scope," which in turn suggested that the recordation software did more than just the ordinary function of a tape recorder; "thus there was a question of fact as to how different it was." *Id.* at *9-10.

In *Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891 (N.D. Cal. 2023), Judge Breyer applied a different analysis. The defendants in the case were Assurance, an insurance website operator, and ActiveProspect, a software provider. Assurance partnered with ActiveProspect so that Assurance could use ActiveProspect's software for its insurance website. Through the software, Assurance was able to record a user's interaction on its website which would allow it to, *e.g.*, document consumer consent. *See id.* at 894-95.

The plaintiff, an individual who used the Assurance website, argued that the defendants had violated § 631 – specifically, ActiveProspect had violated prong (2) and Assurance, by employing ActiveProspect and using its software, prong (4). The defendants argued that the § 631 claim against them should be dismissed because "'ActiveProspect acted solely as an extension of Assurance and therefore was not a third party within the meaning of Section 631.'" *Id.* at 897.

Judge Breyer sided with the plaintiff. He identified two problems with the "extension" theory offered by the defendants.

> The first is that it interprets the second prong of [§ 631] – "willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit" – based on the intentions and usage of the prospective third party. But the third prong of the statute already penalizes "use" – "us[ing], or attempt[ing] to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained." Thus, reading a use requirement into the second prong would add requirements that are not present (and swallow the third prong in the process). The second problem with this view is that it was not the California Supreme Court's stated rationale in *Ribas*: The *Ribas* Court did not consider the wife's friend's intentions or the use to which they put the information they obtained. Instead, it emphasized the privacy concerns at issue with having an "unannounced second auditor" listening in on the call, when Section 631 concerns "the right to control the nature and extent of the firsthand dissemination of [their] statements."

Id. at 900.

Judge Breyer went on to note that one could conclude that ActiveProspect was not an "'unannounced second auditor' of the interaction between [the plaintiff] and Assurance" if ActiveProspect did "not have the *capability* to use its record of the interaction for any other purpose (just as a tape recorder has no independent capability to divulge the recording for any other purpose but that of its owner)." *Id.* (emphasis in original). However, the plaintiff had alleged that ActiveProspect "can use [the] information for other purposes, even if [the plaintiff] has not alleged that [it] has done so in this case." *Id.*

The Court finds the analysis of Judges Beeler and Alsup persuasive for the most part. It also finds that Judge Breyer's reasoning is not wholly inconsistent with that of Judges Alsup and Beeler. The key is whether the hiring of a third party to collect information – even if for the benefit of the contracting party – poses a materially enhanced risk to the individual's privacy. When one considers whether a third party is more like the tape recorder in *Rogers* (no liability) or the friend in *Ribas* (liability), for instance, there is less risk that the individual's privacy will be compromised with a tape recorder because the party holding the tape recorder has control over the tape recorder. In contrast, with the friend in *Ribas*, there was a greater risk that the individual's privacy will be compromised because the friend was not subject to the control of the party who allowed the friend to listen in. *See Ribas*, 38 Cal. 3d at 360-61. Even in *Javier*, Judge Breyer acknowledged the risk that the third party could use the information gathered for other purposes.

Thus, in the case at bar, the critical question is the extent the third parties were subject to Kaiser's control and ability to limit the use of dissemination of the medical data. For instance, what steps did Kaiser take to ensure that third parties could collect and/or use information for Kaiser's benefit only, and not for the benefit of the third parties (*e.g.*, to sell to others)?

To the extent Plaintiffs argue that a third party should *per se* be considered an eavesdropper – *i.e.*, even if hired by a party to the communication to do work solely for the party's benefit and with strict limits on the ability of the third party to use the information for any other purpose – the Court does not agree since that would be inconsistent with the case law discussed above. In this respect, the Court notes that even HIPAA allows a covered entity to disclose

protected information to a "business associate" in certain circumstances. *See* 45 C.F.R. § 164.502(e)(1)(i) ("A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information."); *id.* § 164.504(e)(2)(i)(B) ("The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity"). To be sure, CIPA and HIPAA are distinct statutory schemes. Nevertheless, HIPAA – which has the stated purpose of protecting a patient's right to the confidentiality of his or medical information, *see United States v. Mize*, No. 1:19-CR-00153-3-NODJ-BAM, 2023 U.S. Dist. LEXIS 229192 (E.D. Cal. Dec. 26, 2023) – still provides a meaningful benchmark by which to assess Plaintiffs' position on the CIPA claim.

Accordingly, should Plaintiffs amend to add in a new California Plaintiff to "replace" John Doe, they should bear in mind the Court's views on CIPA as stated above.

G. Count 3: Claim for Common Law Invasion of Privacy – Intrusion Upon Seclusion

In Count 3, Plaintiffs assert a claim for common law invasion of privacy, *i.e.*, intrusion upon seclusion. The claim is a multistate class claim (on behalf of the Kaiser Operating States Class). In the alternative, Plaintiffs assert a claim based on six individual state subclasses (California, D.C., Georgia, Maryland, Oregon, and Washington). As a frame of reference, in California, a claim for intrusion of seclusion has two elements: "(1) [an intentional] intrusion into a private place, conversation or matter [*e.g.*, a person's private affairs or concerns], (2) in a manner highly offensive to a reasonable person." *Taus v. Loftus*, 40 Cal. 4th 683, 725 (2007).

Kaiser argues that the claim for intrusion for seclusion should be dismissed for two reasons: (1) Plaintiffs have asserted that Kaiser violated their privacy rights by disclosing their personal health information to third parties, but a disclosure is not the same thing as an intrusion under any applicable state law; and (2) applicable state law requires that any alleged misconduct be highly offensive and, as a matter of law, Kaiser's conduct does not meet that threshold when all it has allegedly done is hire third parties to do a job (collect information) that it legally could have done itself.

With respect to the first argument, there are cases that have differentiated between intrusions and disclosure when it comes to privacy rights. *See, e.g., ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co.*, 147 Cal. App. 4th 137, 148-49 (2007) (noting that "a person claiming the privacy right of seclusion asserts the right to be free, in a particular location, from disturbance by others," whereas "[a] person claiming the privacy right of secrecy asserts the right to prevent disclosure of personal information to others[;] [i]nvasion of the privacy right of seclusion involves the *means, manner, and method* of communication in a location (or at a time) which disturbs the recipient's seclusion," while "invasion of the privacy right of secrecy involves the *content* of communication that occurs when someone's private, personal information is disclosed to a third person") (emphasis in original). But for purposes of the instant case, that differentiation does not matter. Plaintiffs have alleged not only disclosure but also intrusion via interception.

Kaiser's second argument, however, has merit. As discussed above, there are no allegations that Kaiser knew and/or approved of third parties collecting and/or using information for their own purposes (and not for the limited purpose of Kaiser's use). Therefore, the Court is presented with a situation where Kaiser simply hired a third party to do work for Kaiser's own benefit and with no showing that Kaiser did so in a way that materially increases the risk of dissemination of the collected information. Given the current allegations, it is not clear how that is highly offensive to a reasonable person in light of the above discussion in connection with CIPA.

The Court therefore dismisses the claim for intrusion upon seclusion but with leave to amend.

H. Count 4: Claim for Invasion of Privacy and Violation of the California Constitution

In Count 4, Plaintiffs assert a multistate class claim for invasion of privacy based on the California Constitution. Alternatively, Plaintiffs assert a claim for a California subclass.

In its motion to dismiss, Kaiser makes the same arguments as it did above with respect to the claim for intrusion upon seclusion. *See* Mot. at 22; *see also In re Facebook, Inc.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019) (stating that the analysis of a claim for intrusion on private affairs and a claim for violation of the constitutional right to privacy "is functionally identical, even

though each claim is described somewhat differently in the case law[;] '[w]hen both claims are present, courts conduct a combined inquiry that considers (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification or other relevant interests'"). Accordingly, as above, the Court dismisses the constitutional privacy claim but with leave to amend.

I. Count 5: Claim for Breach of Express Contract

In Count 5, Plaintiffs assert a claim for breach of contract on behalf of the Kaiser Operating States Class (*i.e.*, a multistate class). Alternatively, Plaintiffs assert a breach-of-contract claim on behalf of seven state subclasses (California, D.C., Georgia, Maryland, Oregon, Virginia, and Washington). As a frame of reference, in California, the elements of breach of contract are as follows: "(1) the contract, (2) plaintiff's performance or excuse for nonperformance, (3) defendant's breach, and (4) the resulting damages to plaintiff." *Tribeca Cos., LLC v. First Am. Title Ins. Co.*, 239 Cal. App. 4th 1088, 1109 (2015) (internal quotation marks omitted). In the instant case, the contract that was allegedly breached is the TAC for use of the Kaiser website and mobile applications, which includes the related Privacy Statement.

Kaiser challenges the contract claim on various grounds: (1) there was no breach of contract because Plaintiffs consented to the disclosure of information to the third parties; (2) Plaintiffs have not identified a provision in the TAC that was breached; and (3) to the extent Plaintiffs claim there was a promise to comply with HIPAA, they have failed to show a failure to comply with the statute.

Regarding the argument in (1), the issue of consent has been discussed above. There are factual issues underlying the interpretation of the consent provision.

With respect to (2), here, Kaiser's argument has merit. That is, Plaintiffs claim that certain statements made in the Privacy Statement constituted promises that were breached but Plaintiffs rely on statements that are taken out of context. For example:

- In ¶ 333 of the FAC, Plaintiffs allege that Kaiser warranted in the Privacy Statement that its "data collection 'is collected on an aggregate basis, which means that no personally identifiable information is associated with the data.'" However,

the full statement in the Privacy Statement (under the heading "Site visitor data") is as follows: "In addition to web logs, described below, Kaiser Permanente routinely gathers data on Site activity, such as how many people visit the Site, the web pages or mobile screens they visit, where they come from, how long they stay, etc. The data is collected on an aggregate basis, which means that no personally identifiable information is associated with the data. This data helps us improve our content and overall usage. The information is not shared with other organizations for their independent use. [¶] The Site does not honor a browser's signal or header request not to track the user's activity." FAC, Ex. 2 (Priv. St. at 2-3). Plaintiffs do not explain how this specific promise was breached.

- In ¶ 335, Plaintiffs suggest that Kaiser's use of cookies does not involve the collection of health history. However, the full statement in the Privacy Statement (under the subheading "Internet cookies") is as follows: "We and our service providers may place Internet 'cookies' or similar technologies (JavaScript, HTML5, ETag), on the computer hard drives of visitors to the State. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. The cookie consists of a unique identifier that does not contain information about your health history. . . ." FAC, Ex. 2 (Priv. St. § 3). Plaintiffs do not explain how this specific promise was breached, particularly given that what a cookie consists of is something different from what a cookie does (in terms of collecting and transmitting).
- In ¶ 338, Plaintiffs suggest that Kaiser promises not to "'collect any personally identifiable information about visitors to the Site. The policies, sources, uses and disclosures of information are outlined in Sections 1 through 20 that follow.'" FAC ¶ 338. However, the full statement in the Privacy Statement is as follows: "*Except* as disclosed in this Privacy Statement, we do not collect any personally

identifiable information about visitors to the Site. The policies, sources, uses and disclosures of information are outlined in Sections 1 through 20 that follow." FAC, Ex. 2 (Priv. St. at 3) (emphasis added). Plaintiffs do not clearly explain how this promise was breached.

As for the argument in (3), Kaiser seems to acknowledge that a promise to comply with HIPAA could be inferred from the following statement in the Privacy Statement: "Our use and disclosure of an individual's personal information (including health information) is limited as required by state and federal law." FAC, Ex. 2 (Priv. St. at 2); *see also* FAC, Ex. 2 (Priv. St. at 1-2) ("All of your protected health information maintained by Kaiser Permanente, including information you provide on the Site, is also subject to the Notices of Privacy Practices issued by KP under the [HIPAA]. The Notices of Privacy Practices may contain additional provisions relating to the use and disclosure of your information that go beyond the terms of this Privacy Statement."). Assuming this was tantamount to a promise to comply with HIPAA, Kaiser argues that there are insufficient allegations that it actually violated HIPAA by disclosing HIPAA-protected information. *See* Reply at 10-11.

HIPAA protects against disclosure of "individually identifiable health information." 42 U.S.C. § 1320d-6(a).

> The term "individually identifiable health information" means any information, including demographic information collected from an individual, that –
>
> (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and –
>
> (i) *identifies the individual*; or
> (ii) with respect to which there is a reasonable basis to believe that the information *can be used to identify the individual*.

Id. § 1320d(6) (emphasis added); *see also* 45 C.F.R. § 160.103.

According to Kaiser, "[t]he FAC fails to allege facts sufficient to show that any information Defendants allegedly disclosed to Vendors was identifiable as to one of the Plaintiffs,

or could be linked to Plaintiffs' identities." Reply at 11. The Court agrees. As the FAC is pled, there are no clear allegations as to how individually identifiable health information was disclosed, particularly as to *each* different third party. The fact that third parties may have assigned unique identifiers to individuals using the Kaiser website and mobile applications (*i.e.*, so that they could be tracked) does not in and of itself mean that those individuals' actual *identities* could be divined.

The Court therefore dismisses the claim for breach of contract, but with leave to amend.

J. Count 6: Claim for Breach of Implied Contract

In Count 6, Plaintiffs assert a claim for breach of implied contract on behalf of the Kaiser Operating States Class (*i.e.*, a multistate class). Alternatively, Plaintiffs assert a breach-of-implied-contract claim on behalf of seven state subclasses (California, D.C., Georgia, Maryland, Oregon, Virginia, and Washington). As a frame of reference, in California, "[a] cause of action for breach of implied contract has the same elements as does a cause of action for breach of contract, except that the promise is not expressed in words but is implied from the promisor's conduct." *Yari v. Producers Guild of America, Inc.*, 161 Cal. App. 4th 172, 182 (2008); *see also Green Valley Landowners Ass'n v. City of Vallejo*, 241 Cal. App. 4th 425, 433 (2015) (noting that "[t]he terms of an express contract are stated in words" whereas "[t]he existence and terms of an implied contract are manifested by conduct[;] [t]he distinction reflects no difference in legal effect but merely in the mode of manifesting assent") (internal quotation marks omitted).

In the instant case, Plaintiffs allege that there was an implied contract between Kaiser and members/users where Kaiser

> offered to provide . . . what it represented to be a secure Portal and secure mobile applications through which [members/users] could confidentially make appointments, review medical history, [etc.] and [members/users] agreed to use the purportedly secure Portal and mobile applications to make appointments, view medical history, [etc.] instead of doing so by other means, such as by phone or in person.

FAC ¶ 359. According to Plaintiffs, this implied contract "was created by virtue of the relationship and conduct of the parties [*e.g.*, a confidential health care provider/patient relationship], as well as the surrounding circumstances." FAC ¶ 360. Plaintiffs allege that Kaiser breached the implied contract by disclosing to third parties members/users' "patient status,

personally identifiable data, and confidential communications . . . made within the patient Portal and mobile applications, thereby failing to provide . . . the secure site and mobile applications it agreed to provide." FAC ¶ 366.

In its motion, Kaiser argues that the implied contract should be dismissed because, as pled in the FAC, there was an express contract between Kaiser and its members/users that governed the exact subject matter. "'[A]n action based on an implied-in-fact [contract] . . . cannot lie where there exists between the parties a valid express contract covering the same subject matter.'" *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1095 (N.D. Cal. 2022). In *Hammerling*, the court noted that the plaintiffs had "clearly allege[d] that they had an enforceable contract with Google; indeed, they cite[d] and quote[d] from the Terms of Service and Privacy Policy throughout their complaint. Moreover, these documents also govern[ed] the subject matter of Plaintiffs' implied contract claim – scope and purpose of data collection." *Id.* at 1095-96.

In response, Plaintiffs do not dispute the law above but simply argue that "the federal rules permit [them] to plead relief in the alternative." Opp'n at 28; *see also SocialApps, LLC v. Zynga, Inc.*, No. 4:11-CV-04910 YGR, 2012 U.S. Dist. LEXIS 14124, at *8 (N.D. Cal. Feb. 6, 2012) ("While the allegations of the implied contract claim rely on the same allegations as the express contract claim, SA is entitled to plead different theories of recovery in the alternative."). Kaiser quibbles in its reply, arguing that the implied contract claim was not expressly pled in the alternative. *See* Reply at 12. This is an argument of form over substance. The Court therefore denies the motion to dismiss the claim for breach of implied contract.[7]

K. Count 7: Claim for Negligence Per Se

In Count 7, Plaintiffs bring a claim for "negligence per se" on behalf of the Kaiser Operating States Class. In the alternative, they assert a claim on behalf of seven state subclasses (California, D.C., Georgia, Maryland, Oregon, Virginia, and Washington). As a frame of reference, in California, "[t]he elements of a negligence cause of action are duty, breach, causation, and damages." *Coyle v. Historic Mission Inn Corp.*, 24 Cal. App. 5th 627, 634 (2018).

[7] Neither party asserts the laws of other states entail a materially different analysis.

Furthermore, "[u]nder the doctrine of negligence per se, compliance with the standard of conduct established by the relevant statute, ordinance, or regulation is adopted as the duty of care. This creates a rebuttable presumption of negligence where the statute, ordinance, or regulation is violated." *Jones v. Awad*, 39 Cal. App. 5th 1200, 1210 (2019). In the instant case, Plaintiffs allege that Kaiser's failure to comply with multiple federal and state statutes – such as the ECPA, HIPAA, state wiretapping laws, state computer crime statutes, state insurance information statutes, and so forth – "constitutes negligence per se." FAC ¶ 385.

In its motion, Kaiser argues that the negligence per se claim fails for three reasons: "(1) negligence per se is not a separate cause of action; (2) intentional conduct cannot support a negligence claim; and (3) Plaintiffs fail to plead injury and damages." Mot. at 25. Because there is no substantive argument made in support of (3), the Court need only consider (1) and (2).

The Court rejects the argument in (1). The argument in (1) elevates form over substance. Even if negligence per se is not a separate cause of action, negligence is, and Kaiser fails to explain why the claim cannot simply be construed as a negligence claim.

As for the argument in (2), it presents a closer call. Kaiser does cite cases noting that "intentional conduct cannot support a claim for negligence." *Lam v. Target Corp.*, No. 2:15-CV-01922-KJM-CKD, 2017 U.S. Dist. LEXIS 152365, at *24 (E.D. Cal. Sept. 19, 2017) (addressing claims for intentional and negligence infliction of emotional distress); *see also Jones v. NVR Inc.*, No. 20-453 (CKK), 2020 U.S. Dist. LEXIS 75133, at *17 (D.D.C. Apr. 29, 2020) (in addressing claim for negligent misrepresentation, stating that "[i]ntentional conduct cannot form the basis of a negligence claim"); *Rega v. Georgia*, No. CV 115-087, 2016 WL 1317693, at *4 (S.D. Ga. Apr. 1, 2016) (stating that, "[u]nder Georgia law, negligence denotes unintentional acts, not intentional acts such as discrimination," and "negligence is not a surrogate for employment discrimination claims"), *report and recommendation adopted by* 2016 WL 1756912 (S.D. Ga. Apr. 29, 2016); *Schuerholz v. Coker*, No. WMN-15-1990, 2016 U.S. Dist. LEXIS 150190, at *9 (D. Md. Oct. 31, 2016) (in suit related to arrest by the police, noting that "negligence is not an intentional tort but, instead, arises where an individual's unintentional failure to use reasonable care results in injury to another," but, "[h]ere, Plaintiff is clearly alleging intentional conduct"); *Hartman v. Brady*, No.

3:15-cv-1753-AC, 2016 U.S. Dist. LEXIS 144923, at *14-15 (D. Or. Sept. 19, 2016) (stating that, "[i]n Oregon, 'intentional conduct does not support a claim for negligence under Oregon law," and, therefore, "to the extent plaintiff alleges [defendants] are negligent (through its officers) for arresting plaintiff, his claim fails because plaintiff attempts to category an intentional tort as negligent conduct and rests his negligence claim on the same factual allegations as his constitutional claim"); *Witcher v. Reid*, 70 Va. Cir. 415, 419 (2006) (agreeing that a claim that a defendant negligently or innocently misrepresented a fact is a legal impossibility because "negligence is not an intentional tort").

However, as noted above, a per se negligence claim can be based on a violation of statute. Kaiser has not demonstrated that all of the statutory claims brought by Plaintiffs are not viable, and therefore there is room for a negligence claim even if some statutory claims may be dismissed.[8]

Accordingly, the motion to dismiss the negligence claim is denied.[9]

L. Count 8: Claim for Violation of the California Consumer Legal Remedies Act

In Count 8, Plaintiffs assert a claim for violation of the California Consumer Legal Remedies Act ("CLRA"), either on behalf of a multistate class or, in the alternative, on behalf of a California subclass. The CLRA provides that certain "unfair methods of competition and unfair or deceptive acts or practices . . . undertaken by any person in a transaction intended to result or that results in the sale or lease of goods or services to any consumer are unlawful." Cal. Civ. Code § 1770(a). Illegal conduct includes "(5) [r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have" and "(16) [r]epresenting that the subject of a transaction has been supplied in accordance with a previous representation when it has not." *Id.* § 1770(a)(5), (16). Here, Plaintiffs allege that the CLRA was

[8] To the extent the laws of states other than California are at issue, Kaiser does not contend that these states' laws do not recognize the negligence per se doctrine and/or that the analysis under these laws differs materially from that under California law.

[9] That being said, as noted above, at this juncture, Plaintiffs do not seem to argue that Kaiser negligently failed to ensure that third parties could not use information collected from Kaiser plan members for their own benefit (as opposed to Kaiser's).

violated because, in essence, Kaiser did not comply with the TAC for use of the website and mobile applications, which includes the related Privacy Statement. *See, e.g.*, FAC ¶ 395 (alleging that Kaiser has engaged in deceptive trade practices by allowing "unauthorized interception, disclosure, and transfer of private health information in violation of its own Site Terms and Conditions").

In its motion, Kaiser makes a number of arguments: (1) Plaintiffs have failed to plead detrimental reliance; (2) CLRA liability is limited to transactions involving the actual or contemplated sale or lease of goods and services, and Plaintiffs' use of the website and mobile applications did not involve such transactions; (3) the CLRA applies to misrepresentations about goods or services but the website and mobile applications are neither goods nor services as defined by the statute; and (4) Plaintiffs are not consumers for purposes of the CLRA because they did not use the website or mobile applications with the intention of making a purchase of any goods or services. The arguments in (2)-(4) somewhat overlap and are the primary focus of Kaiser's briefs.

In their opposition, Plaintiffs respond to the primary argument as follows: "There is no requirement that Plaintiffs allege that they made a purchase through the Site or Apps as plaintiffs are consumers engaged in qualified transactions." Opp'n at 30.

Plaintiffs, however, seem to have missed the point. The gist of a CLRA claim is that a misrepresentation was made "in a transaction intended to result or that results in the sale or lease of goods or services to any consumer." Cal. Civ. Code § 1770(a). Even if misrepresentations were made in the TAC or related Privacy Statement, there is no clear allegation that they were made in the context of a transaction intended to result or resulting in the sale or lease of goods or services. Plaintiffs were *already* Kaiser members – *i.e.*, had already purchased health care insurance with Kaiser. While a website and mobile applications can be services covered by the CLRA, the alleged representations made in the TAC or related Privacy Statement were not intended to result in the purchase of website/mobile application services from Kaiser to those who were already members.

The cases cited by Plaintiffs in their opposition are distinguishable because, in those cases, the plaintiffs did allege that misrepresentations or omissions were made that affected their

decisions to purchase goods or services from the defendants. *See, e.g.*, *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 313 F. Supp. 3d 1113, 1140 (N.D. Cal. 2018) (taking note of plaintiff's allegations that Yahoo represented to users that their accounts were secure when in fact it did not use appropriate safeguards to protect users' personal information which had led to that information being exposed to hackers who infiltrated Yahoo's systems; had Yahoo" disclosed the data breaches, "the significant media and expert attention would have alerted Plaintiff . . . and he would not have provided his PII or signed up for Yahoo's services"); *In re iPhone App. Litig.*, 844 F. Supp. 2d 1040, 1049-50 1070-71 (N.D. Cal. 2012) (taking note of plaintiffs' allegations that Apple made representations about precautions taken to protect device users' personal information, and, therefore, "Plaintiffs did not expect or consent to the tracking and collecting of their app use or otherwise personal information"; the true cost of the "free apps" meant that plaintiffs had overpaid for the devices). No such similar allegation is made here.

Accordingly, the CLRA claim is dismissed but with leave to amend.[10]

M. Count 9: Claim for Violation of the California Confidentiality of Medical Information Act

In Count 9, Plaintiffs assert a claim for violation of the California Confidentiality of Medical Information Act ("CMIA"), either on behalf of a multistate class or on behalf of a California subclass. The CMIA is similar to HIPAA, protecting against disclosure of individually identifiable medical information without written, signed authorization.

> "The basic scheme of the [Confidentiality Act], as amended in 1981, is that a provider of health care must not disclose medical information without a written authorization from the patient." "The 'authorization' requirements, which are found in section 56.11, are detailed and demanding, reflecting the Legislature's interest in assuring that medical information may be disclosed only for a narrowly defined purpose, to an identified party, for a limited period of time." Alternatively, disclosure will be permitted if the provider "can show that the disclosure is excepted either by the mandatory ([Cal. Civ. Code] § 56.10, subd. (b)) or permissive (§ 56.10[, subd. (c)]) provisions of the act, allowing disclosure of medical information under specified circumstances."

Brown v. Mortensen, 51 Cal. 4th 1052, 1070-71 (2011).

[10] The Court notes that Kaiser did not raise an argument that the CLRA claim could be asserted by a California plaintiff only. The Court therefore does not address the issue in this order.

In its motion to dismiss, Kaiser makes three arguments related to the CMIA claim: (1) Plaintiffs have failed to allege that individually identifiable medical information was disclosed to third parties; (2) Plaintiffs have failed to plead economic loss or personal injury as a result of any disclosure; and (3) at most, only Kaiser plan members from California have a CIMA claim, and not any non-California members/users.

Regarding the argument in (3), Kaiser is making the same kind of choice-of-law argument that it did with the CIPA claim. *See* Mot. at 29 (arguing that the laws of each member/user's home state applies; that there are material differences between the law of California and the laws of other states (*e.g.*, what constitutes consent, what remedies are available); and that the home state has the "predominant interest in determining how to regulate and protect the medical privacy of their residents"). The parties essentially incorporate their arguments on the CIPA claim here. Thus, the Court rules on the CMIA claim just as it ruled on the CIPA claim: only a California Plaintiff may bring a CMIA claim, and, because the Court compelled John Doe to arbitration, there is no California Plaintiff to assert the CMIA claim.

In addition, the Court finds merit to Kaiser's argument in (1) above. Count 5 involved the same basic issue regarding individually identifiable information.

The CMIA claim is therefore dismissed but with leave to amend.

N. Count 10: Claim for Statutory Larceny

In Count 10, Plaintiffs allege a claim for statutory larceny, predicated on the California Penal Code (specifically, §§ 484 and 496). The claim is asserted on behalf of a multistate class or, in the alternative, a California subclass. Section 496(a) makes it unlawful for a person to

> buy[] or receive[] any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or [to] conceal[], sell[], withhold[], or aid[] in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained.

Cal. Pen. Code § 496(a); *see also id.* § 496(c) (providing that a person injured by a violation of § 496(a) "may bring an action for three times the amount of actual damages, if any, sustained by the plaintiff, costs of suit, and reasonable attorney's fees"). Section 484 defines what constitutes theft:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person, obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

Id. § 484(a).

According to Plaintiffs, Kaiser "acted in a [manner] constituting theft . . . through its installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications, allowing it to, without consent and contrary to its representations in its Terms and Conditions, appropriate or acquire through fraud [members/users'] private health information." FAC ¶ 420.

In its motion, Kaiser makes two arguments: (1) Plaintiffs have failed to plead statutory larceny because statutory larceny requires a trespassory taking; and (2) there can be no kind of theft when Plaintiffs "voluntarily and intentionally transmitted information to Defendants through the Site and Apps." Mot. at 30.

On (1), Plaintiffs argue that, even though they have titled their claim "statutory *larceny*," their claim is really one for theft by false pretenses, which like larceny falls under the rubric of § 484(a). *See generally People v. Williams*, 57 Cal. 4th 776, 785-86 (2013) (noting that "many state legislatures [including California's], recognizing the burdens imposed on prosecutors by the separation of the three crimes of larceny, false pretenses, and embezzlement, consolidated those offenses into a single crime, called 'theft'"; for theft, one can "simply allege an unlawful taking") (internal quotation marks omitted). In *Williams*, the California Supreme Court noted that "larceny requires asportation, which is a carrying away of stolen property," while theft by false pretenses has no such requirement. *Id.* at 787 (internal quotation marks omitted). Theft by false pretenses simply requires that "(1) the defendant made a false pretense or representation to the owner of property; (2) with the intent to defraud the owner of that property; and (3) the owner transferred the property to the defendant in reliance on the representation." *Id.* (internal quotation marks

omitted).

But even if the Court liberally construes the "larceny" claim as one for theft by false pretenses, it is not clear how there is theft if Kaiser only authorized third parties to collect information for Kaiser's benefit, and not for the third parties' own use. For the reasons stated above, just as there is no unlawful interception, there is no "theft" when Kaiser who has the authority to collect information, hires a third party to do its work, provided that information is assuredly not used for any other purposes. Further, as noted above, there is no allegation in the FAC that Kaiser knew or approved of the use of member information by third parties for their benefit, as opposed to Kaiser's.

The claim for theft by false pretenses, therefore, is dismissed, although with leave to amend.[11]

O. Count 11: Claim for Violation of the District of Columbia Consumer Protection Procedures Act

Count 11 is brought by Jane Doe II only on behalf of a D.C. subclass. The claim asserted is violation of the D.C. Consumer Protection Procedures Act ("DCCPPA"). Under the DCCPPA, it is unlawful "to engage in an unfair or deceptive trade practice, whether or not any consumer is in fact misled, deceived, or damages thereby," which includes:

- "(a) represent[ing] that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have";
- "(e) misrepresent[ing] as to a material fact which has a tendency to mislead";
- "(f) failing to state a material fact if such failure tends to mislead"; and
- "(f-1) us[ing] innuendo or ambiguity as to a material fact, which has a tendency to mislead."

D.C. Code § 28-3904(a), (e), (f), (f-1). Jane Doe II alleges that Kaiser engaged in a deceptive trade practice by installing third-party code on its website and mobile applications which allowed

[11] Similar to above, Kaiser did not raise an argument that the claim for theft could be asserted by a California plaintiff only. The Court therefore does not address the issue in this order.

it to intercept private health information without a Kaiser plan member's consent and "contrary to [the] Terms and Conditions." FAC ¶ 429.

Kaiser argues that the DCCPPA claim should be dismissed because such a claim cannot be based on a breach of contract, even if the breach is intentional, and, here, Jane Doe II has pointed to a contract, *i.e.*, the TAC. *See* Mot. at 31. In support, Kaiser cites, *inter alia*, *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1 (D.D.C. 2019), which noted that a run-of-the-mill breach of contract does not constitute an unlawful trade practice under the DCCPPA. *Attias* implies that a run-of-the-mill breach is not a violation of the statute because that would make all breaches a statutory violation. *See id.* (noting that plaintiffs did not cite any authority to support the proposition that "the mere breach of contract constitutes an unlawful trade practice under the DCCPPA"). The *Attias* court also stated that even an intentional breach of contract "is not punishable as an unlawful trade practice . . . simply because the breach was intended when the contract was formed" – *e.g.*, that the defendant stated it would comply with its Internet Privacy Policy "knowing full well that it would not." *Id.* at 26 (internal quotation marks omitted). In support of this statement, *Attias* cited *Slinski v. Bank of America, N.A.*, 981 F. Supp. 2d 19 (D.D.C. 2013), where the court noted that, under D.C. common law, an

> intentional breach is no different than simple breach unless the breaching party's conduct assumes the character of a willful tort, in which case the claim for breach merges with that tort, and punitive damages are allowed. The [DCCPPA], on the other hand, affords a panoply of strong remedies, including treble damages, punitive damages and attorneys' fees, to consumers who are victimized by unlawful trade practices.

Id. at 35 (internal quotation marks omitted). The *Slinski* court continued: "To accept the plaintiffs' argument that an intentional breach of contract is punishable as an unlawful trade practice if the breach was intended when the contract was formed[, . . .] the court would have to conclude that the [DCCPPA] has substantially revised the District's common law of contract." *Id.*

In response, Jane Doe II cites *Sere v. Group Hospitalization, Inc.*, 443 A.2d 33 (D.C. Ct. App. 1982). In *Sere*, the court stated that, ordinarily, punitive damages are not available for a breach of contract even if the breach was "willful, wanton, or malicious. . . . [O]nly where the alleged breach of contract 'merges with, and assumes the character of, a willful tort' will punitive

damages be available. More precisely, the breach must merge with and assume the character of a willful tort." *Id.* at 37.

The primary question, then, is whether Jane Doe II has alleged more than just, *e.g.*, a run-of-the-mill breach or an intent to breach at the time of contract formation and has alleged instead something more along the lines of an intentional tort. Here, the Court is not convinced that, as the FAC is pled, Plaintiffs have sufficiently met this standard. As noted above, there is no allegation that Kaiser allowed the third parties to intercept information for anyone's benefit other than Kaiser. Without such allegations, similar to the reasoning discussed above, it is not clear how Kaiser misled Kaiser plan members – *i.e.*, it was simply hiring third parties to do what it legally could have done itself. Plaintiffs cite no case law interpreting the DCCPPA to the contrary. That being the case, the Court concludes that, as the FAC stands, Plaintiffs have pled at most something more akin to a run-of-the-mill breach.

The DCCPPA claim is dismissed but with leave to amend.

P. Count 12: Claim for Violation of the Georgia Uniform Deceptive Trade Practices Act

In Count 12, John Doe II asserts a claim on behalf of a Georgia subclass for violation of the Georgia Uniform Deceptive Trade Practices Act ("GUDTPA"). In support of this claim, he alleges as follows:

> 436. The Georgia Uniform Deceptive Trade Practices Act (GUDTPA) provides that "a person engages in a deceptive trade practice when, in the course of his business, vocation, or occupation, he . . . Represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he does not have;" or "Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code Ann. § 10-1-372(a)(5), (12).
>
> 437. Kaiser Permanente's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Georgia Sub-Class to the Third Party Wiretappers is a deceptive trade practices under Ga. Code Ann. § 10-1-372.

FAC ¶¶ 436-37. "Injunctive relief is the sole remedy under the UDTPA." *Willingham v. Global*

Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *54 (N.D. Ga. Feb. 5, 2013).

In its motion, Kaiser contends that the GUDTPA claim should be dismissed because John Doe II has failed to allege that he *relied* on any misrepresentation by Kaiser. *See id.* at *5 (stating that "Plaintiffs have not pled that they read, relied upon and, thus, were harmed by Defendants' 'representations'"). The Court agrees there is no clear allegation that John Doe II read the TAC (including the related Privacy Statement) and thus relied on it, and accordingly dismisses the claim. However, dismissal is with leave to amend.

Q. Count 13: Violation of the Georgia Computer Systems Protection Act

In Count 13, John Doe II asserts a claim on behalf of a Georgia subclass for violation of the Georgia Computer Systems Protection Act ("GCSPA"). He points to two provisions in the statute in particular:

- *Computer theft.* A person is guilty of the crime of computer theft if the person "uses a computer or computer network with knowledge that such use is *without authority* and with the intention of: (1) Taking or appropriating any property of another, whether or not with the intention of depriving the owner of possession; (2) Obtaining property by any deceitful means or artful practice; or (3) Converting property to such person's use in violation of an agreement or other known legal obligation to make a specified application or disposition of such property." Ga. Code Ann. § 16-9-93(a) (emphasis added).
- *Computer invasion of privacy.* A person is guilty of the crime of computer invasion of privacy if the person "uses a computer or computer network with the intention of examining any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination is *without authority*." *Id.* § 16-9-93(c) (emphasis added).

The phrase "without authority" is defined to "*include*[] the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." *Id.* § 16-9-92(18) (emphasis added). According to John Doe II, Kaiser

committed computer theft and computer invasion of privacy because it installed third-party code on its website and mobile applications that intercepted private medical information, without his consent and contrary to the TAC (including the related Privacy Statement).

Kaiser asserts that the GCSPA claim should be dismissed because (1) it did not act "without authority" and (2) John Doe has failed to allege a connection to Georgia (*i.e.*, the GCSPA cannot apply extraterritorially).

The Court is skeptical of the second argument because Kaiser cannot have it both ways: for other claims, Kaiser argues that the interception takes place where the Kaiser plan member's home state/residence is, and John Doe II is a Georgia resident. However, the Court need not rule on the second argument because the first argument has merit. Plaintiffs have failed to adequately allege that Kaiser acted without authority; as the FAC stands, Kaiser has simply hired third parties to do work for the benefit of Kaiser which Kaiser legally could have done itself. Nothing in the contract expressly prohibits Kaiser from contracting out work it could have done itself without violating law.

The GCSPA claim is therefore dismissed but with leave to amend.

R. Count 14: Claim for Violation of the Georgia Insurance and Information Privacy Protection Act

In Count 14, John Doe II asserts a claim on behalf of a Georgia subclass for violation of the Georgia Insurance and Information Privacy Protection Act ("GIIPPA"). He cites in particular Georgia Code Annotated § 33-39-14 which provides in relevant part as follows: "An insurance institution, agent, or insurance-support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is (1) With the written authorization of the individual . . . ." Ga. Code Ann. § 33-39-14(1). He alleges that this provision was violated when Kaiser installed third-party code on its website and mobile applications that allowed the interception of members/users' personal or privileged information without authorization. *See* FAC ¶ 459.

As an initial matter, John Doe II seems to concede that a GIIPPA claim is viable against only KFHP. *See* FAC ¶ 457 (alleging that KFHP "is an insurance institution under the Act");

Opp'n at 35 n.27 (noting that the only defendant identified in the heading for Count 14 is KFHP).

That leaves Kaiser with the following arguments on the GIIPPA claim: (1) John Doe II has failed to allege that there was a disclosure "in connection with an insurance transaction" and (2) John Doe II has failed to allege that individually identifiable personal or privileged information was disclosed.

As to (1), the Court looks first to what an "insurance transaction" is in the first place.

> "Insurance transaction" means any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs which entails:
>
> (A) The individual determination of an individual's eligibility for an insurance coverage, benefit, or payment; or
>
> (B) The servicing of an insurance application, policy, contract, or certificate.

Ga. Code Ann. § 33-39-3(13). Given (B) above, which is stated in fairly broad terms, Kaiser's argument that the "in connection with an insurance transaction" requirement has not been met is quibbling. Servicing an insurance policy would include the services provided through the website and mobile applications in common parlance. Kaiser has cited no authority to the contrary.

As for (2), the GIIPPA provides protection for both personal information and privileged information.

- "'Personal information' means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. 'Personal information does not include an individual's name, address, and age when no other underwriting information is gathered on that individual nor does it include any 'privileged information.'" *Id.* § 33-39-3(19).
- "'Privileged information' means any individually identifiable information that: (A) Relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual; and (B) Is collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an

> individual; provided, however, that information otherwise meeting the requirements of this paragraph shall nevertheless be considered 'personal information' under this chapter if it is disclosed in violation of Code Section 33-39-14." *Id.* § 33-39-3(22).

Given that the definition of "personal information" is fairly broad in nature, the only issue is whether John Doe II has explained how *individually identifiable* personal information was disclosed. This is the same issue that has been discussed above, *e.g.* in conjunction with the claim for breach of express contract. As the FAC is pled, there is no clear allegation as to how individually identifiable personal information was disclosed, particularly as to each different third party.

Accordingly, the Court dismisses the GIIPPA claim but with leave to amend.

S. Count 15: Claim for Violation of the Maryland Wiretapping and Electronic Surveillance Act

In Count 15, Jane Doe III asserts on behalf of a Maryland subclass a claim for violation of the Maryland Wiretapping and Electronic Surveillance Act ("MWESA"). Under the statute, it is unlawful:

- For any person to "[w]illfully intercept, indeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral or electronic communication," Md. Code Ann., Cts. & Jud. Proc. § 10-402(a)(1); and
- For a person or entity providing an electronic communication service to the public to "intentionally divulge the contents of any communication (other than one to the person or entity providing the service, or an agent of the person or entity) while in transmission on that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient." *Id.* § 10-402(d)(1).

In its motion, Kaiser argues that the MWESA claim should be dismissed because the statute does not have an extraterritorial effect. However, Jane Doe III has alleged that she is a Maryland resident; thus, it can be fairly be inferred that any interception took place in her home

state of Maryland. As noted above, Kaiser cannot have it both ways; for other claims, it has argued that the interception should be deemed in the Kaiser plan member's home state. The motion to dismiss the MWESA claim is therefore denied.

T. Count 16: Claim for Violation of the Oregon Unlawful Trade Practices Act

In Count 16, Jane Doe V asserts on behalf of an Oregon subclass a claim for violation of the Oregon Unlawful Trade Practices Act ("OUTPA"). She alleges as follows:

> 487. The Oregon Unlawful Trade Practices Act provides that "[a] person engages in an unlawful practice if in the course of the person's business, vocation or occupation the person does any of the following:" (1) [r]epresents that real estate, goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, quantities or qualities that the real estate, goods or services do not have," or (2) "[e]ngages in any other unfair or deceptive conduct in trade or commerce." Or. Rev. Stat. § 646.608(e), (u).
>
> 488. Kaiser Permanente's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Oregon Sub-Class to the Third Party Wiretappers is an unlawful trade practice under Or. Rev. Stat. § 646.607(1).

FAC ¶¶ 487-88.

Kaiser takes issue with the OUTPA claim because Jane Doe V cited § 646.607(1) in ¶ 488 above. Section 646.607(1) provides that "[a] person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person: (1) Employs an unconscionable tactic in connection with selling, renting or disposing of real estate, goods or services, or collecting or enforcing an obligation." Or. Rev. Stat. § 646.607(1). Kaiser argues that a claim for violation of § 646.607 can be brought by the state of Oregon only. *See, e.g., Horton v.* Nelson, 252 Or. App. 611, 619 (2012) ("[O]nly the state can prosecute trade practices declared unlawful by ORS 646.607. . . . The UTPA also includes a private enforcement provision, ORS 646.638(1), which allows individuals to enforce UTPA violations.").

In response, Jane Doe V essentially admits that she cannot proceed under § 646.607. However, she notes that she also referenced § 646.608 in her FAC and, under § 646.638(1),

> [e]xcept as provided in subsections (8) and (9) of this section, a person that suffers an ascertainable loss of money or property, real or personal, as a result of another person's willful use or employment of a method, act or practice declared unlawful under ORS 646.608, may bring an individual action in an appropriate court to recover actual damages or statutory damages of $200, whichever is greater. The court or the jury may award punitive damages and the court may provide any equitable relief the court considers necessary or proper.

Or. Rev. Stat. § 646.638(1).

Thus, to the extent Jane Doe V has cited § 646.607(1), she has no viable claim, but her citation to § 646.608 does give rise to a viable claim. That Jane Doe V did not specifically reference § 646.638(1) does not count against her; ruling otherwise would elevate form over substance.

The motion to dismiss the OUTPA claim is therefore denied.

U. Count 17: Claim for Violation of the Virginia Computer Crimes Act

In Count 17, Jane Doe IV asserts a claim for violation of the Virginia Computer Crimes Act ("VCCA") on behalf of a Virginia subclass. She cites in particular the following provisions from the statute:

> It is unlawful for any person, with malicious intent, or through intentionally deceptive means and without authority, to:
>
> . . . .
>
> 6. Use a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by, or produced by a computer or computer network;
>
> . . . .
>
> 8. Install or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another.

Va. Code Ann. § 18.2152.1 *et seq.* Jane Doe alleges that both of these provisions were violated when Kaiser installed third-party code that intercepted private health information without authorization and contrary to the Terms and Conditions. *See* FAC ¶¶ 498-99.

In its motion, Kaiser argues the VCCA claim should be dismissed because Jane Doe IV

has failed to allege that (1) Kaiser had the requisite intent and (2) Kaiser lacked authority. Both of these issues go back to the question of whether Kaiser acted improperly by hiring a third party to do work that it could have done legally itself, particularly if Kaiser took steps to protect to limit the use of the information collected. Again, Plaintiffs cite no authority suggesting the applicability of a different analysis.

The Court therefore dismisses the VCCA claim but with leave to amend.

V. Count 18: Claim for Violation of the Virginia Insurance Information and Privacy Protection Act

In Count 18, Jane Doe IV asserts a claim on behalf of a Virginia subclass for violation of the Virginia Insurance Information and Privacy Protection Act ("VIIPPA"). The statute generally provides that "[a]n insurance institution, agent, or insurance-support organization shall not disclose any medical-record information or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written authorization of the individual . . . ." Va. Code Ann. § 38.2-613(A). Jane Doe IV alleges: "Kaiser Permanente's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization, disclose Plaintiffs' and Virginia Sub-Class members' personal or privileged information to the Third Party Wiretappers is a violation of Va. Code Ann. § 38.2-613(A)." FAC ¶ 509.

Kaiser moves to dismiss the VIIPPA claim on the basis that Jane Doe IV has failed to allege collection of information "in connection with an insurance transaction." This issue has already been addressed above in conjunction with the analogous claim under Georgia law. *See* Va. Code Ann. § 38.2-602 (defining insurance transaction as, *e.g.*, "any transaction involving insurance primarily for personal, family, or household needs rather than business or professional needs that entails: . . . 2. The servicing of an insurance application, policy, contract, or certificate").

The motion to dismiss the VIIPPA claim is denied.

W. Count 19: Claim for Violation of the Washington Consumer Protection Act

In Count 19, Jane Doe asserts on behalf of a Washington subclass a claim for violation of

the Washington Consumer Protection Act ("WCPA"). Under the WCPA, "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." Wash. Rev. Code. § 19.86.020. The Washington Supreme Court has stated that the elements of a WCPA claim are as follows: (1) an unfair or deceptive act or practice; (2) in trade or commerce; (3) which affects the public interest; (4) that injures a plaintiff in his or her business or property; and (5) causation (*i.e.*, a causal link between the unfair or deceptive act and the injury suffered). *See Hangman Ridge Training Stables v. Safeco Title Ins. Co.*, 105 Wash. 2d 778, 784-85 (1986).

Jane Doe alleges that

> Kaiser Permanente's installation of the Third Party Wiretappers' code on its website, Patient Portal, and mobile applications allowing it to, without authorization and contrary to its representation in the Site Terms and Conditions, intercept, disclose, and transfer private health information belonging to Plaintiff and members of the Washington Sub-Class to the Third Party Wiretappers is an unfair or deceptive act or practice under Wash. Rev. Code § 19.86.020.

FAC ¶ 517.

Kaiser challenges the WCPA claim on various grounds. First, it argues that Jane Doe has failed to allege an improper act "in the conduct of any trade or commerce." This argument is not persuasive as the terms "trade" and "commerce" are defined broadly. "'Trade' and 'commerce' shall *include* the sale of assets or services, and any commerce directly or indirectly affecting the people of the state of Washington." Wash. Rev. Code § 19.86.010(2). Here, Jane Doe is suing the website and mobile applications as a part of getting health care services; that is sufficient to fall under statute even if the use of the website and mobile applications was not necessarily to purchase services.

Second, Kaiser argues that Jane Doe has failed to make any allegations that the conduct at issue affects the public interest. Regarding the public interest factor, the Washington Supreme Court has noted as follows:

> whether the public has an interest in any given action is to be determined by the trier of fact from several factors, depending upon the context in which the alleged acts were committed. Where the

> transaction was essentially a consumer transaction, *see, e.g.*, *Haner v. Quincy Farm Chems., Inc.*, 97 Wn.2d 753 (1982) (plaintiff farmer purchased defective wheat seed); *Lidstrand v. Silvercrest Indus.*, 28 Wn. App. 359 (1981) (plaintiff purchased defective mobile home); *Dempsey v. Joe Pignataro Chevrolet, Inc.*, 22 Wn. App. 384 (1979) (plaintiff purchased new automobile with defective paint job); *Testo v. Russ Dunmire Oldsmobile, Inc.*, 16 Wn. App. 39 (1976) (plaintiff purchased defective used automobile), these factors are relevant to establish public interest: (1) Were the alleged acts committed in the course of defendant's business? (2) Are the acts part of a pattern or generalized course of conduct? (3) Were repeated acts committed prior to the act involving plaintiff? (4) Is there a real and substantial potential for repetition of defendant's conduct after the act involving plaintiff? (5) If the act complained of involved a single transaction, were many consumers affected or likely to be affected by it?
>
> Where the transaction was essentially a private dispute (*see, e.g.*, *Lightfoot v. MacDonald*, *supra* (attorney-client); *Short v. Demopolis*, 103 Wn.2d 52 (1984) (attorney-client); *Salois v. Mutual of Omaha Ins. Co.*, 90 Wn.2d 355 (1978) (**insurer-insured**); *McRae v. Bolstad*, 101 Wn.2d 161 (1984) (realtor-property purchaser); *Bowers v. Transamerica Title Ins. Co.*, 100 Wn.2d 581 (escrow closing agent-client)), it may be more difficult to show that the public has an interest in the subject matter. Ordinarily, a breach of a private contract affecting no one but the parties to the contract is not an act or practice affecting the public interest. *Lightfoot v. MacDonald*, *supra* at 334. However, it is the likelihood that additional plaintiffs have been or will be injured in exactly the same fashion that changes a factual pattern from a private dispute to one that affects the public interest. *McRae v. Bolstad*, *supra* at 166. Factors indicating public interest in this context include: (1) Were the alleged acts committed in the course of defendant's business? (2) Did defendant advertise to the public in general? (3) Did defendant actively solicit this particular plaintiff, indicating potential solicitation of others? (4) Did plaintiff and defendant occupy unequal bargaining positions? As with the factors applied to essentially consumer transactions, not one of these factors is dispositive, nor is it necessary that all be present. The factors in both the "consumer" and "private dispute" contexts represent indicia of an effect on public interest from which a trier of fact could reasonably find public interest impact.
>
> In addition to the above method of establishing public interest, . . . the public interest element may be satisfied per se. The per se method requires a showing that a statute has been violated which contains a specific legislative declaration of public interest impact.

Hangman Ridge Training Stables, 105 Wash. 2d at 789-91 (emphasis added).

Here, even though Jane Doe does not specifically included allegations about impact on the public interest, she has challenged a practice regarding the website and mobile applications that affects more than just herself.

Finally, Kaiser argues that Jane Doe has failed to make allegations about injury (to

business or property) and the causal link between the conduct challenged and the injury. In response, Jane Doe argues that her injury is the "depriv[ation] of the full value of her personal health information." Opp'n at 38. She also alleges the following in the FAC:

> 221. Kaiser Plan Members' confidential communications and information that Kaiser Permanente allows the Third Party Wiretappers to intercept has monetary value.
>
> 222. For example, one recent study asked over a thousand consumers from around the world what price they would demand of third parties for access to their data and found that passwords would fetch $75.80; health information and medical records themselves average $59.80; and in third, Social Security numbers were valued at $55.70.45
>
> 223. Some companies, such as Prognos Health, sell what they purport to be de-identified health information from millions of patients.
>
> 224. Due to the difficulty in obtaining health information, illegal markets also exist for such data, with some reporting that health data can be "more expensive than stolen credit card numbers."

FAC ¶¶ 221-24. In light of the above, Jane Doe has pled enough allegations to support a claim of injury to property.

Accordingly, the specific arguments raised by Kaiser above all lack merit. The motion to dismiss the WCPA claim is denied.

X. Count 20: Claim for Violation of the Washington Privacy Act

In Count 20, Jane Doe brings a claim on behalf of a Washington subclass for violation of the Washington Privacy Act ("WPA"). The WPA provides in relevant part:

> it shall be unlawful for any individual, partnership, corporation, association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any:
>
> (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication . . . .

Wash. Rev. Code § 9.73.030(1)(a).

In its motion to dismiss, Kaiser makes three arguments: (1) Jane Doe has failed to allege a communication between two or more individuals; (2) Kaiser was a party to the communications; and (3) Jane Doe has failed to allege an injury to her business, person, or reputation, which is required even if all that is sought is statutory damages.

Regarding (1), Kaiser is correct in noting that courts (including this one) have rejected WPA claims on the grounds that there were not communications involving *individuals*. *See, e.g.*, *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012) ("[I]f [defendant] Microsoft intercepted [plaintiff] Cousineau's communication, as she argues, with whom was Cousineau communicating? Without an individual on the other end of her communication (other than Microsoft), the [mere] transmission of Cousineau's data cannot be considered a communication under the WPA."); *In re Carrier IQ, Inc., Consumer Privacy Litig.*, 78 F. Supp. 3d 1051, 1093 (N.D. Cal. 2015) ("[T]he Court finds that Plaintiffs may base their Washington Privacy Act claim on the alleged interception of text messages and phone numbers dialed and received. Such information reflects communications 'between two or more individuals' and therefore fits within Washington's definition of interception. The alleged interception of other data – such as user's geographical location, URLs, search terms, etc. – may not form the basis for liability under Washington's Privacy Act as this data was not transmitted as part of a communication between individuals but instead directed to an automated system.").

Jane Doe responds that she nevertheless has a claim because among the information intercepted by third parties was communication between her health care providers and herself (*e.g.*, "messages sent via the Message Center"). Opp'n at 38; *see also* FAC ¶ 2 (alleging that the website and mobile applications can be used, *e.g.*, to "exchange messages and healthcare information with providers"); FAC ¶¶ 60-61 (describing a Message Center in the patient portal); FAC ¶¶ 93, 98 (alleging that, when *John* Doe used the Message Center, information was intercepted by Quantum Metric and that "the communications of members of the Classes who accessed the Kaiser Permanente website and Patient Portal were also intercepted by Quantum Metric"). Kaiser contends that there is no clear allegation that Jane Doe used the Message Center – *i.e.*, that ¶ 93 addresses use of the Message Center by *John* Doe instead. However, given that all

reasonable inferences are to be made in Jane Doe's favor, it is fair to read ¶ 98 as alleging that she too, like John Doe used the Message Center.

As for (2), Kaiser makes a fair point that, as a party to the communication, it could not intercept. *See Hoang v. Amazon.com, Inc.*, No. C11-1709 MJP, 2012 U.S. Dist. LEXIS 45498, at *15 (W.D. Wash. Mar. 28, 2012) (stating that the statute did not apply because, "regardless of what [Defendants] did with [Plaintiff's] information, Defendants were the intended recipients of the communication"). Jane Doe argues that the interception was done by third parties, and not Kaiser itself and that the WPA contains a provision stating: "Any person who, directly or by means of a detective agency *or any other agent*, violates the provisions of this chapter shall be subject to legal action for damages . . . ." Wash. Rev. Code § 9.73.060 (emphasis added). But even if the third parties are Kaiser's agents, that does not detract from Kaiser's status as a party to the communication if what was done was pursuant to Kaiser's directive. If anything, this simply takes the Court back to the question of whether Kaiser can be held liable for hiring a third party to do work that Kaiser could have legally done itself. Again, Jane Doe cites no Washington authority suggesting a different analysis on this question.

Finally, on (3), the WPA provides for relief where a violation has injured a plaintiff's

> business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation.

Id. Kaiser contends that Jane Doe has not suffered any injury to business, person, or reputation but instead is relying simply on the alleged invasion of privacy as the injury. *See Jones v. Ford Motor Co.*, 85 F.4th 570, 575 (9th Cir. 2023) ("[A]n invasion of privacy, without more, is insufficient to meet the statutory injury requirements of Section 9.73.060. To succeed at the pleading stage of a WPA claim, Plaintiffs must allege an injury to 'his or her business, his or her person, or his or her reputation.'"). However, it is not clear why Jane Doe cannot claim as an injury to her person a deprivation of her right to monetize her personal health information as noted above.

Accordingly, based on the above, although two of Kaiser's arguments are not persuasive, at least one is. Accordingly, the Court dismisses the WPA claim but with leave to amend.

Y. Count 21: Claim for Violation of the Washington Health Care Information Act

In Count 21, Jane Doe asserts a claim on behalf of a Washington subclass for violation of the Washington Health Care Information Act ("WHCIA"). Under the statute,

> a health care provider, an individual who assists a health care provider in the delivery of health care, or an agent and employee of a health care provider may not disclose health care information about a patient to any other person without the patient's written authorization. A disclosure made under a patient's written authorization must conform to the authorization.

Wash. Rev. Code § 70.02.020(1). "Health care information" is defined as follows:

> any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information.

Id. § 70.02.010(17).

Here, Kaiser argues once again that there is no allegation that individually identifiable information has been disclosed. Jane Doe, in response, has cited to one paragraph suggesting that individually identifiable information may have been disclosed to Quantum Metric, *see* FAC ¶ 86 (alleging that, when she logged into the portal, her name, medical record number (Kaiser ID number), etc. were displayed and that information was transferred to Quantum Metric), but even that allegation is not altogether clear. Moreover, there is no explanation of how there was disclosure of individually identifiable information with respect to other third parties. Although Jane Doe has made allegations that information was disclosed to other third parties and that third parties could track her use of the website and mobile applications, *see* Opp'n at 40 (citing FAC ¶¶ 117, 119-23, 126, 130, 142, 152, 155, 181-88, 209-11), it is not clearly alleged that such information identified her or could be readily associated with her personal identity.

The Court therefore grants the motion to dismiss the WHCIA claim but with leave to amend.

IV. CONCLUSION

For the foregoing reasons, the Court hereby grants in part and denies in part Kaiser's motion to dismiss. Specifically:

- The motion to dismiss John Doe II and Jane Does II-V is denied.
- The motion to dismiss Hospitals and TPMG is granted.
- The Court denies the motion to the dismiss to the extent Kaiser argues that consent may be determined on a blanket-wide basis.
- The motion to dismiss the ECPA claim is granted.
- The motion to dismiss the CIPA claim is granted.
- The motion to dismiss the claim for intrusion upon seclusion is granted.
- The motion to dismiss the claim for violation of privacy as protected by the California Constitution is granted.
- The motion to dismiss the claim for breach of express contract is granted.
- The motion to dismiss the claim for breach of implied contract is denied.
- The motion to dismiss the negligence claim is denied.
- The motion to dismiss the CLRA claim is granted.
- The motion to dismiss the CMIA claim is granted.
- The motion to dismiss the claim for theft by false pretenses is granted.
- The motion to dismiss the DCCPPA claim is granted.
- The motion to dismiss the GUDTPA claim is granted.
- The motion to dismiss the GCSPA claim is granted.
- The motion to dismiss the GIIPPA claim is granted.
- The motion to dismiss the MWESA claim is denied.
- The motion to dismiss the OUTPA claim is denied.
- The motion to dismiss the VCCA claim is granted.
- The motion to dismiss the VIIPPA claim is denied.
- The motion to dismiss the WCPA claim is denied.
- The motion to dismiss the WPA claim is granted.

- The motion to dismiss the WHCA claim is granted.

Plaintiffs have leave to amend on dismissed claims. The second amended complaint ("SAC") shall be filed by May 9, 2024. Kaiser shall then have until June 6, 2024, to file a response to the SAC, whether the response is an answer or another motion to dismiss. If Plaintiffs do not file a SAC by the specified deadline, then Kaiser shall have June 6, 2024, to file an answer to the FAC.

This order disposes of Docket No. 88.

IT IS SO ORDERED.

Dated: April 11, 2024

EDWARD M. CHEN
United States District Judge

United States District Court
Northern District of California